Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Dublin 17.10.x

First Published: 2022-11-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xcvii

Document Conventions xcvii

Related Documentation xcix

Communications, Services, and Additional Information xcix

Cisco Bug Search Tool xcix

Documentation Feedback xcix

CHAPTER 1

Overview of the Controller 1

Overview of Cisco 9800 Series Wireless Controllers 1

Elements of the New Configuration Model 1

Configuration Workflow 2

Initial Setup 3

Interactive Help 4

PART I

System Configuration 7

CHAPTER 2

New Configuration Model 9

Information About New Configuration Model 9

Configuring a Wireless Profile Policy (GUI) 12

Configuring a Wireless Profile Policy (CLI) 12

Configuring a Flex Profile (GUI) 14

Configuring a Flex Profile 14

Configuring an AP Profile (GUI) 15

Configuring an AP Profile (CLI) 20

Configuring User for AP Management (CLI) 21

Setting a Private Configuration Key for Password Encryption 21

Configuring an RF Profile (GUI) 22
Configuring an RF Profile (CLI) 22
Configuring a Site Tag (GUI) 24
Configuring a Site Tag (CLI) 24
Enhanced Site Tag-Based Load Balancing 25
Feature History for Enhanced Site Tag-Based Load Balancing 25
Information About Enhanced Site Tag-Based Load Balancing 26
Prerequisites for Enhanced Site Tag-Based Load Balancing 26
Use Cases 27
Configuring Site Load (CLI) 27
Verifying Enhanced Site Tag-Based Load Balancing Configuration 27
Configuring Policy Tag (GUI) 28
Configuring a Policy Tag (CLI) 28
Configuring Wireless RF Tag (GUI) 29
Configuring Wireless RF Tag (CLI) 30
Attaching a Policy Tag and Site Tag to an AP (GUI) 31
Attaching Policy Tag and Site Tag to an AP (CLI) 31
Configuring a Radio Profile 32
Information About Wireless Radio Profile 32
Configuring a Wireless Radio Profile (GUI) 33
Configuring a Radio Profile and Beam Selection 34
Configuring the Antenna Count in a Wireless Radio Profile 34
Configuring a Slot Per Radio in the RF Tag Profile 35
Verifying a Radio Profile 35
AP Filter 36
Introduction to AP Filter 36
Set Tag Priority (GUI) 37
Set Tag Priority 37
Create an AP Filter (GUI) 38
Create an AP Filter (CLI) 38
Set Up and Update Filter Priority (GUI) 39
Set Up and Update Filter Priority 39
Verify AP Filter Configuration 40
Configuring Access Point for Location Configuration 41

Information About Location Configuration 41
Prerequisite for Location Configuration 41
Configuring a Location for an Access Point (GUI) 41
Configuring a Location for an Access Point (CLI) 42
Adding an Access Point to the Location (GUI) 42
Adding an Access Point to the Location (CLI) 43
Configuring SNMP in Location Configuration 44
SNMP MIB 44
Verifying Location Configuration 44
Verifying Location Statistics 45

CHAPTER 3 **Wireless Management Interface** 47
Information About Wireless Management Interface 47
Recommendations for Wireless Management Interface 48
Configuring your Controller with Wireless Management Interface (CLI) 49
Verifying Wireless Management Interface Settings 51
Information About Network Address Translation (NAT) 52
Information About CAPWAP Discovery 52
Configuring Wireless Management Interface with a NAT Public IP (CLI) 53
Configuring CAPWAP Discovery to Respond Only with Public or Private IP (CLI) 54
Configuring the Controller to Respond only with a Public IP (CLI) 54
Configuring the Controller to Respond only with a Private IP (CLI) 54
Verifying NAT Settings 55

CHAPTER 4 **BIOS Protection** 57
BIOS Protection on the Controller 57
BIOS or ROMMON Upgrade with BIOS Protection 57
Upgrading BIOS 58

CHAPTER 5 **Smart Licensing Using Policy** 59
Introduction to Smart Licensing Using Policy 59
Information About Smart Licensing Using Policy 60
Overview 60
Supported Products 60

Architecture 61
Product Instance 61
CSLU 61
CSSM 62
Controller 62
SSM On-Prem 63
Concepts 64
License Enforcement Types 64
License Duration 65
Authorization Code 65
Policy 65
RUM Report and Report Acknowledgement 67
Trust Code 68
Supported Topologies 69
Connected to CSSM Through CSLU 69
Connected Directly to CSSM 71
CSLU Disconnected from CSSM 73
Connected to CSSM Through a Controller 74
No Connectivity to CSSM and No CSLU 75
SSM On-Prem Deployment 77
Interactions with Other Features 80
High Availability 80
Upgrades 81
Downgrades 83
How to Configure Smart Licensing Using Policy: Workflows by Topology 86
Workflow for Topology: Connected to CSSM Through CSLU 86
Workflow for Topology: Connected Directly to CSSM 89
Workflow for Topology: CSLU Disconnected from CSSM 90
Workflow for Topology: Connected to CSSM Through a Controller 93
Workflow for Topology: No Connectivity to CSSM and No CSLU 94
Workflow for Topology: SSM On-Prem Deployment 95
Tasks for Product Instance-Initiated Communication 95
Tasks for SSM On-Prem Instance-Initiated Communication 98
Migrating to Smart Licensing Using Policy 100

Example: Smart Licensing to Smart Licensing Using Policy 101
Example: SLR to Smart Licensing Using Policy 108
Example: Evaluation or Expired to Smart Licensing Using Policy 116
Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy 119
Task Library for Smart Licensing Using Policy 121
RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller 121
Logging into Cisco (CSLU Interface) 124
Configuring a Smart Account and a Virtual Account (CSLU Interface) 124
Adding a Product-Initiated Product Instance in CSLU (CSLU Interface) 124
Ensuring Network Reachability for Product Instance-Initiated Communication 125
Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface) 126
Collecting Usage Reports: CSLU Initiated (CSLU Interface) 127
Export to CSSM (CSLU Interface) 128
Import from CSSM (CSLU Interface) 128
Ensuring Network Reachability for CSLU-Initiated Communication 129
Assigning a Smart Account and Virtual Account (SSM On-Prem UI) 133
Validating Devices (SSM On-Prem UI) 133
Ensuring Network Reachability for Product Instance-Initiated Communication 134
Retrieving the Transport URL (SSM On-Prem UI) 137
Exporting and Importing Usage Data (SSM On-Prem UI) 137
Adding One or More Product Instances (SSM On-Prem UI) 138
Ensuring Network Reachability for SSM On-Prem-Initiated Communication 139
Setting Up a Connection to CSSM 144
Configuring Smart Transport Through an HTTPs Proxy 146
Configuring the Call Home Service for Direct Cloud Access 147
Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server 150
Removing and Returning an Authorization Code 151
Removing the Product Instance from CSSM 153
Generating a New Token for a Trust Code from CSSM 154
Installing a Trust Code 155
Downloading a Policy File from CSSM 156
Uploading Data or Requests to CSSM and Downloading a File 157
Installing a File on the Product Instance 158

Setting the Transport Type, URL, and Reporting Interval 159
Configuring an AIR License 162
Sample Resource Utilization Measurement Report 164
Troubleshooting Smart Licensing Using Policy 164
System Message Overview 164
System Messages 166
Additional References for Smart Licensing Using Policy 176
Feature History for Smart Licensing Using Policy 176

CHAPTER 6 **Management over Wireless** 181
Information About Management over Wireless 181
Restrictions on Management over Wireless 181
Enabling Management over Wireless on Controller (GUI) 181
Enabling Management over Wireless on Controller (CLI) 182

CHAPTER 7 **Boot Integrity Visibility** 183
Overview of Boot Integrity Visibility 183
Verifying Software Image and Hardware 183
Verifying Platform Identity and Software Integrity 184

CHAPTER 8 **SUDI99 Certificate Support** 187
SUDI99 Certificate Support 187
Disabling SUDI99 Migration (GUI) 189

CHAPTER 9 **Link Aggregation Group** 191
Information About Link Aggregation Group 191
Link Aggregation Control Protocol 191
Configuring LAG Using LACP 192
Port Aggregation Protocol 192
Configuring LAG Using PAgP 192
Information About Port Channel Interface Number 192
Configuring LAG in ON Mode 193
Multichassis Link Aggregation Group 193
Prerequisites for Multi-LAG 193

Restrictions for Multi-LAG 194
Supported Topologies 194
Configuring a Port Channel Interface (GUI) 195
Create a Port-Channel Interface 196
Configuring LAG in ON Mode 196
Add an Interface to a Port Channel (LACP) 197
Add an Interface to a Port Channel (PAgP) 198
Add a VLAN to a Port Channel 198
Remove a Port Channel Group from a Physical Interface 199
Verify the LAG Configuration 199

CHAPTER 10 Best Practices 201
Introduction 201

PART II System Upgrade 203

CHAPTER 11 Upgrading the Cisco Catalyst 9800 Wireless Controller Software 205
Overview of Upgrading the Controller Software 205
Upgrading the Controller Software (GUI) 206
Upgrade the Controller Software (CLI) 207
Converting From Bundle-Mode to Install-Mode 208
Copying a WebAuth Tar Bundle to the Standby Controller 211

CHAPTER 12 In-Service Software Upgrade 213
Information About In-Service Software Upgrade 213
Prerequisites for Performing In-Service Software Upgrade 214
Guidelines and Restrictions for In-Service Software Upgrade 214
Upgrading Software Using In-Service Software Upgrade 215
Upgrading Software Using ISSU (GUI) 216
Upgrading Software Using In-Service Software Upgrade with Delayed Commit 217
Monitoring In-Service Software Upgrade 218
Troubleshooting ISSU 220

CHAPTER 13 Software Maintenance Upgrade 223

Introduction to Software Maintenance Upgrade 223
Installing a SMU (GUI) 225
Installing SMU 226
Roll Back an Image (GUI) 227
Rollback SMU 227
Deactivate SMU 227
Configuration Examples for SMU 228
Information About AP Device Package 228
Installing AP Device Package (GUI) 229
Installing AP Device Package (CLI) 230
Verifying APDP on the Controller 230
Information About Per Site or Per AP Model Service Pack (APSP) 231
Rolling AP Upgrade 232
Rolling AP Upgrade Process 232
Installing AP Service Package (GUI) 233
Installing AP Service Package (CLI) 234
Adding a Site to a Filter 235
Deactivating an Image 235
Roll Back APSP 236
Canceling the Upgrade 236
Verifying the Upgrade 236
Verifying of AP Upgrade on the Controller 239

CHAPTER 14 **Efficient Image Upgrade** 241
Efficient Image Upgrade 241
Enable Pre-Download (GUI) 241
Enable Pre-Download (CLI) 242
Configuring a Site Tag (CLI) 242
Attaching Policy Tag and Site Tag to an AP (CLI) 243
Trigger Predownload to a Site Tag 244

CHAPTER 15 **Predownloading an Image to an Access Point** 247
Information About Predownloading an Image to an Access Point 247
Restrictions for Predownloading an Image to an Access Point 247

Predownloading an Image to Access Points (CLI) 248
Predownloading an Image to Access Points (GUI) 250
Predownloading an Image to Access Points (YANG) 250
Monitoring the Access Point Predownload Process 251
Information About AP Image Download Time Enhancement (OEAP or Teleworker Only) 252
Configuring AP Image Download Time Enhancement (GUI) 253
Configuring AP Image Download Time Enhancement (CLI) 253
Verifying AP Image Download Time Enhancement Configuration 254

CHAPTER 16 **N+1 Hitless Rolling AP Upgrade** 255
N+1 Hitless Rolling AP Upgrade 255
Configuring Hitless Upgrade 256
Verifying Hitless Upgrade 257

CHAPTER 17 **Site-Based Rolling AP Upgrade in N+1 Networks** 259
Feature History for Site-Based Rolling AP Upgrade in N+1 Networks 259
Information About Site-Based Rolling AP Upgrade in N+1 Network 259
Prerequisites for Site-Based Rolling AP Upgrade in N+1 Networks 260
Restrictions for Site-Based Rolling AP Upgrade in N+1 Networks 260
Use Cases 260
N+1 Upgrade and Move to Destination Controller 261
N+1 Move to Destination Controller 263
Hitless Software Upgrade (N+1 Upgrade) 264
Verifying Site-based Rolling AP Upgrade in a N+1 Network 265

CHAPTER 18 **NBAR Dynamic Protocol Pack Upgrade** 271
NBAR Dynamic Protocol Pack Upgrade 271
Upgrading the NBAR2 Protocol Pack 272

CHAPTER 19 **Wireless Sub-Package for Switch** 273
Introduction to Wireless Sub-package 273
Booting in Install Mode 274
Installing Sub-Package in a Single Step (GUI) 275
Installing Sub-Package in a Single Step 275

Multi-step Installation of Sub-Package 276
Installing on a Stack 276
Upgrading to a Newer Version of Wireless Package 277
Deactivating the Wireless Package 277
Enabling or Disabling Auto-Upgrade 277

PART III **Lightweight Access Points** 279

CHAPTER 20 **Countries and Regulations** 281
Information About Country Codes 281
Prerequisites for Configuring Country Codes 281
Configuring Country Codes (GUI) 282
Configuring Country Codes (CLI) 282
Configuration Examples for Configuring Country Codes 284
Viewing Channel List for Country Codes 284
Information About Regulatory Compliance Domain 285
Global Country-Level Domains 286
Restrictions on Regulatory Compliance Domain 290
Countries Supporting 6-GHz Radio Band 290
Rest of World Domain 297
Configuring Country Code for Rest of the World (CLI) 305

CHAPTER 21 **Access Points Modes** 307
Information about Sniffer 308
Information About XOR Radio Role Sniffer Support 308
Feature History for Sniffer Mode 309
Prerequisites for Sniffer 309
Restrictions on Sniffer 309
How to Configure Sniffer 310
Configuring an Access Point as Sniffer (GUI) 310
Configuring an Access Point as Sniffer (CLI) 311
Enabling or Disabling Sniffing on the Access Point (GUI) 311
Enabling or Disabling Sniffing on the Access Point (CLI) 312
Configuring XOR Radio Role Sniffer Support on the Access Point (CLI) 312

Verifying Sniffer Configurations 313
Verifying XOR Radio Role Sniffer Configuration 314
Examples for Sniffer Configurations and Monitoring 315
Introduction to Monitor Mode 315
Enable Monitor Mode (GUI) 315
Enable Monitor Mode (CLI) 316
Feature History for Management Mode Migration in Cisco Catalyst Wireless 916X Access Points 316
Information About Management Mode Migration in Cisco Catalyst Wireless 916X Series Access Points 317
Regulatory Domain 317
Configuring Management Mode Migration (GUI) 321
Exporting Meraki Management Mode-Migrated APs (GUI) 321
Configuring the AP Management Mode (CLI) 322
Verifying the Management Mode Migration Details 323
Information About FlexConnect 323
FlexConnect Authentication 325
Guidelines and Restrictions for FlexConnect 327
Configuring a Site Tag 331
Configuring a Policy Tag (CLI) 332
Attaching a Policy Tag and a Site Tag to an Access Point (GUI) 333
Attaching Policy Tag and Site Tag to an AP (CLI) 333
Linking an ACL Policy to the Defined ACL (GUI) 334
Applying ACLs on FlexConnect 335
Configuring FlexConnect 336
Configuring a Switch at a Remote Site 336
Configuring the Controller for FlexConnect 337
Configuring Local Switching in FlexConnect Mode (GUI) 337
Configuring Local Switching in FlexConnect Mode (CLI) 338
Configuring Central Switching in FlexConnect Mode (GUI) 338
Configuring Central Switching in FlexConnect Mode 339
Configuring an Access Point for FlexConnect 339
Configuring an Access Point for Local Authentication on a WLAN (GUI) 339
Configuring an Access Point for Local Authentication on a WLAN (CLI) 340
Connecting Client Devices to WLANs 340

Configuring FlexConnect Ethernet Fallback 341
Information About FlexConnect Ethernet Fallback 341
Configuring FlexConnect Ethernet Fallback 341
Flex AP Local Authentication (GUI) 342
Flex AP Local Authentication (CLI) 343
Flex AP Local Authentication with External Radius Server 345
Configuration Example: FlexConnect with Central and Local Authentication 348
NAT-PAT for FlexConnect 348
Configuring NAT-PAT for a WLAN or a Remote LAN 348
Creating a WLAN 348
Configuring a Wireless Profile Policy and NAT-PAT (GUI) 349
Configuring a Wireless Profile Policy and NAT-PAT 349
Mapping a WLAN to a Policy Profile 350
Configuring a Site Tag 351
Attaching a Policy Tag and a Site Tag to an Access Point (GUI) 351
Attaching a Policy Tag and a Site Tag to an Access Point 352
Split Tunneling for FlexConnect 352
Configuring Split Tunneling for a WLAN or Remote LAN 353
Defining an Access Control List for Split Tunneling (GUI) 353
Defining an Access Control List for Split Tunneling 353
Linking an ACL Policy to the Defined ACL 354
Creating a WLAN 355
Configuring a Wireless Profile Policy and a Split MAC ACL Name (GUI) 355
Configuring a Wireless Profile Policy and a Split MAC ACL Name 356
Mapping a WLAN to a Policy Profile (GUI) 357
Mapping WLAN to a Policy Profile 357
Configuring a Site Tag 358
Attaching a Policy Tag and Site Tag to an Access Point 358
VLAN-based Central Switching for FlexConnect 359
Configuring VLAN-based Central Switching (GUI) 359
Configuring VLAN-based Central Switching (CLI) 360
OfficeExtend Access Points for FlexConnect 361
Configuring OfficeExtend Access Points 362
Disabling OfficeExtend Access Point 362

Support for OEAP Personal SSID 363
Information About OEAP Personal SSID Support 363
Configuring OEAP Personal SSID (GUI) 363
Configuring OEAP Personal SSID (CLI) 364
Viewing OEAP Personal SSID Configuration 364
Clearing Personal SSID from an OfficeExtend Access Point 365
Example: Viewing OfficeExtend Configuration 365
Proxy ARP 366
Enabling Proxy ARP for FlexConnect APs (GUI) 366
Enabling Proxy ARP for FlexConnect APs 366
Overlapping Client IP Address in Flex Deployment 367
Overview of Overlapping Client IP Address in Flex Deployment 367
Enabling Overlapping Client IP Address in Flex Deployment (GUI) 367
Enabling Overlapping Client IP Address in Flex Deployment 368
Verifying Overlapping Client IP Address in Flex Deployment (GUI) 368
Verifying Overlapping Client IP Address in Flex Deployment 369
Information About FlexConnect High Scale Mode 370
Enabling PMK Propagation (CLI) 370
Flex Resilient with Flex and Bridge Mode Access Points 371
Information About Flex Resilient with Flex and Bridge Mode Access Points 371
Configuring a Flex Profile (GUI) 371
Configuring a Flex Profile (CLI) 372
Configuring a Site Tag (CLI) 373
Configuring a Mesh Profile (CLI) 373
Associating Wireless Mesh to an AP Profile (CLI) 374
Attaching Site Tag to an Access Point (CLI) 375
Configuring Switch Interface for APs (CLI) 375
Verifying Flex Resilient with Flex and Bridge Mode Access Points Configuration 376
Feature History for OEAP Link Test 376
Information About OEAP Link Test 377
Configuring OEAP Link Test (CLI) 377
Performing OEAP Link Test (GUI) 378
Verifying OEAP Link Test 378
Feature History for Cisco OEAP Split Tunneling 378

Information About Cisco OEAP Split Tunneling 379
Prerequisites for Cisco OEAP Split Tunneling 380
Restrictions for Cisco OEAP Split Tunneling 380
Use Cases for Cisco OEAP Split Tunneling 381
Workflow to Configure Cisco OEAP Split Tunneling 381
Create an IP Address ACL (CLI) 381
Create a URL ACL (CLI) 382
Add an ACL to a FlexConnect Profile 383
Enable Split Tunnelling in a Policy Profile 384
Verifying the Cisco OEAP Split Tunnel Configuration 384
AP Survey Mode 385

CHAPTER 22 **Security** 387
Information About Data Datagram Transport Layer Security 387
Configuring Data DTLS (GUI) 388
Configuring Data DTLS (CLI) 388
Introduction to the 802.1X Authentication 389
EAP-FAST Protocol 390
EAP-TLS/EAP-PEAP Protocol 390
Limitations of the 802.1X Authentication 390
Topology - Overview 391
Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI) 392
Configuring 802.1X Authentication Type and LSC AP Authentication Type 392
Configuring the 802.1X Username and Password (GUI) 393
Configuring the 802.1X Username and Password (CLI) 394
Enabling 802.1X on the Switch Port 394
Verifying 802.1X on the Switch Port 396
Verifying the Authentication Type 397

CHAPTER 23 **AP Joining** 399
Failover Priority for Access Points 399
Setting AP Priority (GUI) 400
Setting AP Priority 400
Overview of Access Point Plug-n-Play 400

Provisioning AP from PnP Server 401
Verifying AP Tag Configuration 401
Feature History for AP Fallback to Controllers Using AP Priming Profile 402
Information About AP Fallback to Controllers Using AP Priming Profile 402
Restrictions for AP Fallback to Controllers Using AP Priming Profile 402
Configure AP Priming Profile 403
Configure AP Priming Using Filters 404
Configure Per-AP Priming 405
Verify the Configuration 405

CHAPTER 24 **AP Management** 407
AP Crash File Upload 408
Configuring AP Crash File Upload (CLI) 409
Information About LED States for Access Points 409
Configuring LED State in Access Points (GUI) 410
Configuring LED State for Access Points in the Global Configuration Mode (CLI) 410
Configuring LED State in the AP Profile 411
Verifying LED State for Access Points 411
Access Point Support Bundle 412
Exporting an AP Support Bundle (GUI) 412
Exporting an AP Support Bundle (CLI) 413
Monitoring the Status of Support Bundle Export 413
Information About Access Point Memory Information 413
Verifying Access Point Memory Information 414
Information About Access Point Tag Persistency 414
Configuring AP Tag Persistency (GUI) 414
Saving Tags on an Access Point (GUI) 415
Deleting Saved Tags on the Access Point 415
Configuring AP Tag Persistency (CLI) 415
Verifying AP Tag Persistency 416
Feature History for AP Power Save 417
Information About AP Power Save 417
Access Point Power Policy 418
Power-Save Mode 418

PoE Profiles 418
Wakeup Threshold for Access Point Power Save Mode 424
AP Power Save Scenarios 424
Configuring Power Policy Profile (GUI) 426
Configuring a Power Policy Profile (CLI) 426
Configuring a Calendar Profile (GUI) 429
Configuring a Calendar Profile (CLI) 430
Configuring a Power Policy in an AP Join Profile (GUI) 431
Mapping a Power Profile Under an AP Profile (CLI) 431
Configuring Client Wakeup Threshold (CLI) 432
Configuring PoE-Out Interface in Power Profile (GUI) 433
Configuring PoE-Out Interface in Power Profile (CLI) 433
Configuration Example of Power Profile 434
Verifying Access Point Power Policy (GUI) 434
435
Verifying the Access Point Power Profile 435
Verifying Radio Spatial Streams 436
Verifying Client Threshold 437
Verifying PoE-Out Details 437
Information About Access Point Real-Time Statistics 437
Feature History for Real Time Access Point Statistics 438
Restrictions for AP Radio Monitoring Statistics 438
Configuring Access Point Real Time Statistics (GUI) 438
Configuring Real-Time Access Point Statistics (CLI) 439
Configuring AP Radio Monitoring Statistics 441
Monitoring Access Point Real-Time Statistics (GUI) 442
Verifying Access Point Real-Time Statistics 443

CHAPTER 25 **AP Configuration** 445

Feature History for Configuring the Access Point Console 446
Information About Configuring the Access Point Console 446
Configuring the AP Console (GUI) 447
Configuring the AP Console (CLI) 447
Verifying the AP Console Status 447

Information About AP Audit Configuration 448
Restrictions for AP Audit Configuration 448
Configure AP Audit Parameters (CLI) 449
Verifying AP Audit Report Summary 449
Verifying AP Audit Report Detail 449
2.4-GHz Radio Support 450
Configuring 2.4-GHz Radio Support for the Specified Slot Number 450
5-GHz Radio Support 452
Configuring 5-GHz Radio Support for the Specified Slot Number 452
6-GHz Radio Support 455
Configuring 6-GHz Radio Support for the Specified Slot Number 455
Information About Dual-Band Radio Support 457
Configuring Default XOR Radio Support 458
Configuring XOR Radio Support for the Specified Slot Number (GUI) 460
Configuring XOR Radio Support for the Specified Slot Number 461
Receiver Only Dual-Band Radio Support 463
Information About Receiver Only Dual-Band Radio Support 463
Configuring Receiver Only Dual-Band Parameters for Access Points 463
Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point (GUI) 463
Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point 463
Disabling Receiver Only Dual-Band Radio on a Cisco Access Point (GUI) 464
Disabling Receiver Only Dual-Band Radio on a Cisco Access Point 464
Configuring Client Steering (CLI) 464
Verifying Cisco Access Points with Dual-Band Radios 466
Information About OFDMA Support for 11ax Access Points 466
Supported Modes on 11ax Access Points 466
Configuring 11AX (GUI) 467
Configuring Channel Width 467
Configuring 802.11ax Radio Parameters (GUI) 468
Configuring 802.11ax Radio Parameters (CLI) 468
Setting up the 802.11ax Radio Parameters 469
Configuring OFDMA on a WLAN 470
Verifying Channel Width 471
Verifying Client Details 472

Verifying Radio Configuration 473
Information About Cisco Flexible Antenna Port 476
Configuring a Cisco Flexible Antenna Port (GUI) 476
Configuring a Cisco Flexible Antenna Port (CLI) 476
Verifying Flexible Antenna Port Configuration 477
Feature History for Environmental Sensors in Access Points 477
Information About Environmental Sensors in Access Points 478
Use Cases 478
Configuring Environmental Sensors in an AP Profile (CLI) 478
Configuring Environment Sensors in Privileged EXEC Mode (CLI) 479
Verifying the AP Sensor Status 480
Information About CAPWAP LAG Support 480
Restrictions for CAPWAP LAG Support 481
Enabling CAPWAP LAG Support on Controller (GUI) 481
Enabling CAPWAP LAG Support on Controller 482
Enabling CAPWAP LAG Globally on Controller 482
Disabling CAPWAP LAG Globally on Controller 482
Enabling CAPWAP LAG for an AP Profile (GUI) 483
Enabling CAPWAP LAG for an AP Profile 483
Disabling CAPWAP LAG for an AP Profile 484
Disabling CAPWAP LAG Support on Controller 484
Verifying CAPWAP LAG Support Configurations 485

CHAPTER 26 **Troubleshooting Lightweight Access Points** 487
Overview 487
Support Articles 487
Feedback Request 488
Disclaimer and Caution 488

PART IV **Radio Resource Management** 489

CHAPTER 27 **Radio Resource Management** 491
Information About Radio Resource Management 491
Radio Resource Monitoring 492

Information About RF Groups 492
RF Group Leader 493
RF Group Name 495
Rogue Access Point Detection in RF Groups 496
Secure RF Groups 496
Transmit Power Control 496
Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings 496
Dynamic Channel Assignment 497
Dynamic Bandwidth Selection 499
Coverage Hole Detection and Correction 499
Cisco AI Enhanced RRM 499
Restrictions for Radio Resource Management 501
How to Configure RRM 502
Configuring Neighbor Discovery Type (GUI) 502
Configuring Neighbor Discovery Type (CLI) 503
Configuring RF Groups 503
Configuring RF Group Selection Mode (GUI) 504
Configuring RF Group Selection Mode (CLI) 504
Configuring an RF Group Name (CLI) 505
Configuring a Secure RF Group (CLI) 505
Configuring Members in an 802.11 Static RF Group (GUI) 506
Configuring Members in an 802.11 Static RF Group (CLI) 506
Configuring Transmit Power Control 507
Configuring Transmit Power (GUI) 507
Configuring the Tx-Power Control Threshold (CLI) 507
Configuring the Tx-Power Level (CLI) 508
Configuring 802.11 RRM Parameters 509
Configuring Advanced 802.11 Channel Assignment Parameters (GUI) 509
Configuring Advanced 802.11 Channel Assignment Parameters (CLI) 511
Configuring 802.11 Coverage Hole Detection (GUI) 513
Configuring 802.11 Coverage Hole Detection (CLI) 513
Configuring 802.11 Event Logging (CLI) 515
Configuring 802.11 Statistics Monitoring (GUI) 516
Configuring 802.11 Statistics Monitoring (CLI) 516

Configuring the 802.11 Performance Profile (GUI) 518
Configuring the 802.11 Performance Profile (CLI) 518
Configuring Advanced 802.11 RRM 519
Enabling Channel Assignment (GUI) 519
Enabling Channel Assignment (CLI) 520
Restarting DCA Operation 520
Updating Power Assignment Parameters (GUI) 521
Updating Power Assignment Parameters (CLI) 521
Configuring Rogue Access Point Detection in RF Groups 521
Configuring Rogue Access Point Detection in RF Groups (CLI) 521
Monitoring RRM Parameters and RF Group Status 523
Monitoring RRM Parameters 523
Verifying RF Group Status (CLI) 523
Examples: RF Group Configuration 524
Information About ED-RRM 524
Configuring ED-RRM on the Cisco Wireless Controller (CLI) 525

CHAPTER 28 **Coverage Hole Detection** 527
Coverage Hole Detection and Correction 527
Configuring Coverage Hole Detection (GUI) 527
Configuring Coverage Hole Detection (CLI) 528
Configuring CHD for RF Tag Profile (GUI) 530
Configuring CHD for RF Profile (CLI) 530

CHAPTER 29 **Optimized Roaming** 533
Optimized Roaming 533
Restrictions for Optimized Roaming 533
Configuring Optimized Roaming (GUI) 534
Configuring Optimized Roaming (CLI) 534

CHAPTER 30 **Cisco Flexible Radio Assignment** 537
Information About Flexible Radio Assignment 537
Configuring an FRA Radio (GUI) 538
Enabling FRA (CLI) 540

Configuring Client FRA in RF Profile (CLI) 542
Verifying FRA XOR 5-GHz and 6-GHz Details 542
Flexible Radio Assignment (FRA) Action 543
Feature History for Flexible Radio Assignment Action 543
Information About Flexible Radio Assignment Action 544
Configuring FRA Action in Default RF Profile (CLI) 544
Configuring FRA Action in 2.4-GHz RF Profile (CLI) 544
Verifying FRA Action Configuration 545

CHAPTER 31 XOR Radio Support 547
Information About Dual-Band Radio Support 547
Configuring Default XOR Radio Support 548
Configuring XOR Radio Support for the Specified Slot Number (GUI) 550
Configuring XOR Radio Support for the Specified Slot Number 551

CHAPTER 32 Cisco Receiver Start of Packet 553
Information About Receiver Start of Packet Detection Threshold 553
Restrictions for Rx SOP 553
Configuring Rx SOP (CLI) 554
Customizing RF Profile (CLI) 554

CHAPTER 33 Client Limit 557
Information About Client Limit 557
Limitations for Client Limit 557
Configuring Client Limit Per WLAN (GUI) 557
Configuring Client Limit Per WLAN (CLI) 558
Configuring Client Limit Per AP (GUI) 559
Configuring Client Limit Per AP (CLI) 559
Configuring Client Limit Per Radio (GUI) 560
Configuring Client Limit Per Radio (CLI) 560
Verifying Client Limit 561

CHAPTER 34 IP Theft 563
Introduction to IP Theft 563

Configuring IP Theft (GUI) 564
Configuring IP Theft 564
Configuring the IP Theft Exclusion Timer 564
Adding Static Entries for Wired Hosts 565
Verifying IP Theft Configuration 566

CHAPTER 35 **Unscheduled Automatic Power Save Delivery** 569
Information About Unscheduled Automatic Power Save Delivery 569
Viewing Unscheduled Automatic Power Save Delivery (CLI) 569

CHAPTER 36 **Target Wake Time** 571
Target Wake Time 571
Extended Power-Savings Using Target Wake Time 571
Configuring Target Wake Time at the Radio Level (CLI) 572
Configuring Target Wake Time on WLAN 573
Enabling Target Wake Time on WLAN (CLI) 573
Disabling Target Wakeup Time on WLAN (CLI) 574
Configuring Target Wake Time (GUI) 575
Verifying Target Wakeup Time 575

CHAPTER 37 **Enabling USB Port on Access Points** 577
USB Port as Power Source for Access Points 577
Configuring an AP Profile (CLI) 578
Configuring USB Settings for an Access Point (CLI) 579
Configuring USB Settings for an Access Point (GUI) 579
Monitoring USB Configurations for Access Points (CLI) 580

CHAPTER 38 **Dynamic Frequency Selection** 581
Feature History for Channel Availability Check (CAC) 581
Information About Dynamic Frequency Selection 581
Information About Channel Availability Check (CAC) 582
Verifying DFS 582
Information About Zero Wait Dynamic Frequency Selection 583
Configuring Zero Wait Dynamic Frequency Selection Globally (CLI) 583

Configuring Zero Wait Dynamic Frequency Selection Globally (GUI) 583
Enabling Zero Wait Dynamic Frequency Selection on a RF Profile (CLI) 584
Enabling Zero Wait Dynamic Frequency Selection on a RF Profile (GUI) 584
Verifying Zero Wait Dynamic Frequency Selection Configuration 585

CHAPTER 39 **Cisco Access Points with Tri-Radio** 587
Cisco Access Points with Tri-Radio 587
Guidelines and Restrictions for Tri-Radio Access Points 589
Configuring Tri-Radio 589
Configuring Tri-Radio for AP (GUI) 589
Configuring the Tri-Radio (CLI) 590
Configuring 5-GHz Dual Radio Mode for AP (GUI) 590
Configuring the Dual Radio Mode and Enabling Slots (CLI) 590
Setting Radio Roles for Slots (CLI) 591
Configuring the Tri-Radio Dual Radio Role (CLI) 591
Verifying Tri-Radio Configuration on the Controller 592

CHAPTER 40 **Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard** 593
Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard 593
Configuring Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard Parameters (CLI) 594
Verifying AP DFS Counters (CLI) 595
Verifying Wi-Fi 6 Access Point Parameters 596

CHAPTER 41 **Antenna Disconnection Detection** 597
Feature History for Antenna Disconnection Detection 597
Information About Antenna Disconnection Detection 597
Recommendations and Limitations 598
Configuring Antenna Disconnection Detection (CLI) 598
Configuring Antenna Disconnection Detection (GUI) 599
Detecting Broken Antenna Using SNMP Trap (CLI) 600
Detecting Broken Antenna Using SNMP Trap (GUI) 600
Verifying Antenna Disconnection Detection 601
Verifying Antenna Disconnection Detection (GUI) 602

CHAPTER 42 Neighbor Discovery Protocol Mode on Access Points 603

Information About Neighbor Discovery Protocol Mode 603

Configuring RRM Neighbor Discovery Mode (GUI) 604

Configuring the Neighbor Discovery Protocol Mode (CLI) 604

Configuring the Neighbor Discovery Protocol Type (CLI) 604

Configuring Neighbor Discovery Protocol Mode in the RF Profile (GUI) 605

Configuring Neighbor Discovery Protocol Mode in the RF Profile (CLI) 605

Monitoring Radio Statistics-NDP Capability and NDP Mode (GUI) 606

Verifying Neighbor Discovery Protocol Mode 607

CHAPTER 43 6-GHz Band Operations 609

Configuring Preferred Scanning Channels in the RF Profile (GUI) 609

Configuring Preferred Scanning Channels in the RF Profile (CLI) 610

Configuring Broadcast Probe Response in RF Profile (GUI) 610

Configuring Broadcast Probe Response in RF Profile (CLI) 610

Configuring FILS Discovery Frames in the RF Profile (GUI) 611

Configuring FILS Discovery Frames in the RF Profile (CLI) 612

Configuring Multi BSSID Profile (GUI) 612

Configuring Multi BSSID Profile 613

Configuring Multi-BSSID in the RF Profile (GUI) 613

Configuring Multi-BSSID in the RF Profile (CLI) 614

Configuring Dynamic Channel Assignment Freeze (CLI) 614

Information About 6-GHz Client Steering 615

Configuring 6-GHz Client Steering in the Global Configuration Mode (GUI) 615

Configuring 6-GHz Client Steering in the Global Configuration Mode 615

Configuring 6-GHz Client Steering on the WLAN (GUI) 616

Configuring 6-GHz Client Steering on the WLAN 617

Verifying 6-GHz Client Steering 617

PART V Network Management 619

CHAPTER 44 AP Packet Capture 621

Introduction to AP Client Packet Capture 621

Enabling Packet Capture (GUI) 621
Enabling Packet Capture (CLI) 622
Create AP Packet Capture Profile and Map to an AP Join Profile (GUI) 622
Create AP Packet Capture Profile and Map to an AP Join Profile 623
Start or Stop Packet Capture 623

CHAPTER 45 DHCP Option82 625
Information About DHCP Option 82 625
Configuring DHCP Option 82 Global Interface 627
Configuring DHCP Option 82 Globally Through Server Override (CLI) 627
Configuring DHCP Option 82 Through Server Override (CLI) 627
Configuring DHCP Option 82 Globally Through Different SVIs (GUI) 628
Configuring DHCP Option 82 Globally Through Different SVIs (CLI) 628
Configuring DHCP Option 82 Format 629
Configuring DHCP Option82 Through a VLAN Interface 630
Configuring DHCP Option 82 Through Option-Insert Command (CLI) 630
Configuring DHCP Option 82 Through the server-ID-override Command (CLI) 631
Configuring DHCP Option 82 Through a Subscriber-ID (CLI) 632
Configuring DHCP Option 82 Through server-ID-override and subscriber-ID Commands (CLI) 633
Configuring DHCP Option 82 Through Different SVIs (CLI) 634

CHAPTER 46 RADIUS Realm 637
Information About RADIUS Realm 637
Enabling RADIUS Realm 638
Configuring Realm to Match the RADIUS Server for Authentication and Accounting 638
Configuring the AAA Policy for a WLAN 639
Verifying the RADIUS-Realm Configuration 641

CHAPTER 47 RADIUS Accounting 643
Information About RADIUS Accounting of AP Events 643
Configuring Accounting Method-List for an AP Profile 643
Verifying the AP Accounting Information 644
AAA Accounting 644
Configuring AAA Accounting Using Default Method List (CLI) 644

Configuring HTTP Command Accounting Using Named Method List (CLI) 645
Feature History for Device Ecosystem Data 645
Information About Device Ecosystem Data 646
Enable Device Ecosystem Data 646
Verify Device Ecosystem Data 647

CHAPTER 48 **RADIUS Call Station Identifier** 649
RADIUS Call Station Identifier 649
Configuring a RADIUS Call Station Identifier 650

CHAPTER 49 **RADIUS VSA** 651
Information About RADIUS VSA 651
Create an Attribute List 652
Create a AAA Policy and Map it to Attribute List 653
Map a AAA Policy to the WLAN Policy Profile 654
Map the WLAN Policy Profile to a WLAN 655

CHAPTER 50 **Cisco StadiumVision** 657
Cisco StadiumVision Overview 657
Configure Parameters for Cisco StadiumVision (GUI) 658
Configure Parameters for Cisco StadiumVision (CLI) 658
Verify StadiumVision Configurations 659

CHAPTER 51 **Persistent SSID Broadcast** 661
Persistent SSID Broadcast 661
Configuring Persistent SSID Broadcast 661
Verifying Persistent SSID Broadcast 662

CHAPTER 52 **Network Monitoring** 663
Network Monitoring 663
Status Information Received Synchronously - Configuration Examples 663
Alarm and Event Information Received Asynchronously - Configuration Examples 665

CHAPTER 53 Creating a Lobby Ambassador Account 667
Information About Lobby Ambassador Account 667
Creating a Lobby Ambassador User Account (GUI) 667
Creating a User Account 668
Logging In Using the Lobby Account 669
Creating a Lobby Ambassador Account (CLI) 669

CHAPTER 54 Lobby Ambassador Account 671
Information About Lobby Ambassador Account 671
Creating a Lobby Ambassador User Account (GUI) 672
Creating a User Account 672
Logging In Using the Lobby Account 673
Creating a Lobby Ambassador Account (CLI) 673
Configuring WLAN (GUI) 674
Client Allowed List 675
Restrictions for Client Allowed List 675
Creating a Client Allowed List (GUI) 675
Adding Single MAC Address to Allowed List 675
Adding Bulk MAC Address to Allowed List 676
Managing Guest Users 676
Viewing a Client Allowed List 677

CHAPTER 55 Guest User Accounts 679
Information About Creating Guest User Accounts 679
Creating a Guest User Account (GUI) 679
Creating a Guest User Account (CLI) 680
Verifying Guest User Account 681
Assigning Username to Guest Users in a WLAN (CLI) 682

CHAPTER 56 Link Local Bridging 683
Feature History for Link Local Bridging 683
Information About Link Local Bridging 683
Use Case for Link Local Bridging 684

Guidelines and Restrictions for Link Local Bridging 684
Enabling Link Local Bridging Per Policy Profile (GUI) 684
Enabling Link Local Bridging Per Policy Profile (CLI) 685
Verifying Link Local Bridging 685

CHAPTER 57 **Web Admin Settings** 687
Information About Web Admin Settings 687
Configuring HTTP/HTTPS Access 687
Configuring HTTP Trust Point 688
Configuring Netconf Yang 689
Configuring Timeout Policy 689
Configuring VTY 690

CHAPTER 58 **Web UI Configuration Command Accounting in TACACS Server** 693
Feature History for Web UI Configuration Command Accounting in TACACS+ Server 693
Information About Web UI Configuration Command Accounting in TACACS+ Server 693
Guidelines for Web UI Configuration Command Accounting in TACACS+ Server 694
Configuring AAA Accounting Using Default Method List (CLI) 694
Configuring HTTP Command Accounting Using Named Method List (CLI) 695

PART VI **System Management** 697

CHAPTER 59 **Network Mobility Services Protocol** 699
Information About Network Mobility Services Protocol 699
Radioactive Tracing for NMSP 700
Enabling NMSP on Premises Services 700
Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues 701
Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues 701
Configuring NMSP Strong Cipher 702
Verifying NMSP Settings 702
Examples: NMSP Settings Configuration 705
NMSP by AP Groups with Subscription List from CMX 705
Verifying NMSP by AP Groups with Subscription List from CMX 705
Probe RSSI Location 707

Configuring Probe RSSI 707
RFID Tag Support 709
Configuring RFID Tag Support 709
Verifying RFID Tag Support 710

CHAPTER 60 **Application Visibility and Control** 713
Information About Application Visibility and Control 713
Prerequisites for Application Visibility and Control 715
Restrictions for Application Visibility and Control 715
AVC Configuration Overview 715
Create a Flow Monitor 716
Configuring a Flow Monitor (GUI) 718
Create a Flow Record 718
Create a Flow Exporter 720
Configuring a Policy Tag 721
Attaching a Policy Profile to a WLAN Interface (GUI) 722
Attaching a Policy Profile to a WLAN Interface (CLI) 722
Attaching a Policy Profile to an AP 723
Verify the AVC Configuration 724
Default DSCP on AVC 725
Configuring Default DSCP for AVC Profile (GUI) 725
Configuring Default DSCP for AVC Profile 725
Creating Class Map 725
Creating Policy Map 726
AVC-Based Selective Reanchoring 727
Restrictions for AVC-Based Selective Reanchoring 728
Configuring the Flow Exporter 728
Configuring the Flow Monitor 728
Configuring the AVC Reanchoring Profile 729
Configuring the Wireless WLAN Profile Policy 730
Verifying AVC Reanchoring 731

CHAPTER 61 **Software-Defined Application Visibility and Control** 735
Information About Software-Defined Application Visibility and Control 735

Enabling Software-Defined Application Visibility and Control on a WLAN (CLI) 736
Configuring Software-Defined Application Visibility and Control Global Parameters (CLI) 736

CHAPTER 62 Cisco Hyperlocation 739
Information About Cisco Hyperlocation 739
Restrictions on Cisco Hyperlocation 741
Support for IPv6 in Cisco Hyperlocation or BLE Configuration 742
Configuring Cisco Hyperlocation (GUI) 742
Configuring Cisco Hyperlocation (CLI) 743
Configuring Hyperlocation BLE Beacon Parameters for AP (GUI) 744
Configuring Hyperlocation BLE Beacon Parameters for AP (CLI) 744
Configuring Hyperlocation BLE Beacon Parameters (CLI) 745
Information About AP Group NTP Server 746
Configuring an AP Group NTP Server 746
Configuring AP Timezone 747
Information About BLE Concurrent Scanning and Beaconing 747
Verifying BLE Concurrent Scanning and Beaconing 748
Verifying Cisco Hyperlocation 749
Verifying Hyperlocation BLE Beacon Configuration 753
Verifying Hyperlocation BLE Beacon Configuration for AP 753

CHAPTER 63 FastLocate for Cisco Catalyst Series Access Points 755
Information About FastLocate 755
Restrictions on FastLocate 755
Supported Access Points 756
FastLocate Network Components 756
Configuring FastLocate (GUI) 757
Verifying FastLocate on Cisco Catalyst APs 757

CHAPTER 64 IoT Services Management 759
Information About IoT Services Management 759
Enabling the Dot15 Radio 760
Configuring the gRPC Token 760
Enabling gRPC in an AP Profile 761

Verifying BLE State and Mode 761
Verifying BLE Details 762
Verifying gRPC Summary, Status, and Statistics 763

CHAPTER 65 IoT Module Management in the Controller 765
Information About IoT Module Management in the Controller 765
Enabling a USB on the Controller 765
Verifying the USB Modules 766

CHAPTER 66 Cisco Spaces 767
Cisco Spaces 767
Configuring Cisco Spaces 767
Verifying Cisco Spaces Configuration 768

CHAPTER 67 EDCA Parameters 771
Enhanced Distributed Channel Access Parameters 771
Configuring EDCA Parameters (GUI) 771
Configuring EDCA Parameters (CLI) 772

CHAPTER 68 Adaptive Client Load-Based EDCA 775
Feature History for Adaptive Client Load-Based EDCA 775
Information About Adaptive Client Load-Based EDCA 775
Restrictions for Adaptive Client Load-Based EDCA 776
Configuration Workflow 776
Configuring Adaptive Client Load-Based EDCA (GUI) 776
Configuring Adaptive Client Load-Based EDCA (CLI) 777
Verifying Adaptive Client Load-Based EDCA Configuration 777

CHAPTER 69 802.11 parameters and Band Selection 779
Information About Configuring Band Selection, 802.11 Bands, and Parameters 779
Band Select 779
802.11 Bands 780
802.11n Parameters 780

802.11h Parameters 780
Restrictions for Band Selection, 802.11 Bands, and Parameters 781
How to Configure 802.11 Bands and Parameters 781
Configuring Band Selection (GUI) 781
Configuring Band Selection (CLI) 782
Configuring the 802.11 Bands (GUI) 783
Configuring the 802.11 Bands (CLI) 784
Configuring a Band-Select RF Profile (GUI) 786
Configuring a Band-Select RF Profile (CLI) 787
Configuring 802.11n Parameters (GUI) 787
Configuring 802.11n Parameters (CLI) 788
Configuring 802.11h Parameters (CLI) 790
Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters 791
Verifying Configuration Settings Using Band Selection and 802.11 Bands Commands 791
Example: Viewing the Configuration Settings for the 6-GHz Band 791
Example: Viewing the Configuration Settings for the 5-GHz Band 793
Example: Viewing the Configuration Settings for the 2.4-GHz Band 794
Example: Viewing the status of 802.11h Parameters 796
Example: Verifying the Band-Selection Settings 796
Configuration Examples for Band Selection, 802.11 Bands, and Parameters 798
Examples: Band Selection Configuration 798
Examples: 802.11 Bands Configuration 799
Examples: 802.11n Configuration 799
Examples: 802.11h Configuration 800

CHAPTER 70 **NBAR Protocol Discovery** 801
Introduction to NBAR Protocol Discovery 801
Configuring NBAR Protocol Discovery 801
Verifying Protocol Discovery Statistics 802

CHAPTER 71 **Conditional Debug, Radioactive Tracing, and Packet Tracing** 803
Introduction to Conditional Debugging 803
Introduction to Radioactive Tracing 804
Conditional Debugging and Radioactive Tracing 804

Location of Tracefiles 805
Configuring Conditional Debugging (GUI) 805
Configuring Conditional Debugging 806
Radioactive Tracing for L2 Multicast 807
Recommended Workflow for Trace files 807
Copying Tracefiles Off the Box 808
Configuration Examples for Conditional Debugging 808
Verifying Conditional Debugging 809
Example: Verifying Radioactive Tracing Log for SISF 809
Information About Packet Tracing 810
Configuring Conditional Debugging Packet Tracing 811
Configuring Conditional Debugging Packet Tracing per AP 812
Configuring Conditional Debugging Packet Tracing per Client (GUI) 813
Configuring Conditional Debugging Packet Tracing per Client 813
Verifying Conditional Debugging Packet Tracing Configuration 813

CHAPTER 72 **Aggressive Client Load Balancing** 815
Information About Aggressive Client Load Balancing 815
Enabling Aggressive Client Load Balancing (GUI) 816
Configuring Aggressive Client Load Balancing (GUI) 816
Configuring Aggressive Client Load Balancing (CLI) 817

CHAPTER 73 **Accounting Identity List** 819
Configuring Accounting Identity List (GUI) 819
Configuring Accounting Identity List (CLI) 819
Configuring Client Accounting (GUI) 820
Configuring Client Accounting (CLI) 820

CHAPTER 74 **Support for Accounting Session ID** 823
Information About Accounting Session ID 823
Configuring an Accounting Session ID (CLI) 823
Verifying an Account Session ID 824

CHAPTER 75 **Interim Accounting** 827

Information About Interim Accounting 827
Disabling Interim Accounting (CLI) 828
Verifying Interim Accounting 828

CHAPTER 76 **Wireless Multicast** 829
Information About Wireless Multicast 829
Multicast Optimization 830
IPv6 Global Policies 830
Information About IPv6 Snooping 830
IPv6 Neighbor Discovery Inspection 830
Prerequisites for Configuring Wireless Multicast 832
Restrictions on Configuring Wireless Multicast 833
Restrictions for IPv6 Snooping 833
Configuring Wireless Multicast 833
Configuring Wireless Multicast-MCMC Mode (CLI) 833
Configuring Wireless Multicast-MCUC Mode 834
Configuring Multicast Listener Discovery Snooping (GUI) 834
Configuring IPv6 MLD Snooping 835
Verifying the Multicast VLAN Configuration 835
IPv6 Multicast-over-Multicast 835
Configuring IPv6 Multicast-over-Multicast (GUI) 836
Configuring IPv6 Multicast-over-Multicast 837
Verifying IPv6 Multicast-over-Multicast 837
Verifying the Multicast Connection Between the Controller and the AP 837
Directed Multicast Service 838
Configuring Directed Multicast Service(GUI) 838
Configuring Directed Multicast Service 838
Verifying the Directed Multicast Service Configuration 839
Wireless Broadcast, Non-IP Multicast and Multicast VLAN 840
Configuring Non-IP Wireless Multicast (CLI) 841
Configuring Wireless Broadcast (GUI) 841
Configuring Wireless Broadcast (CLI) 842
Configuring Multicast-over-Multicast for AP Multicast Groups (CLI) 842
Verifying Wireless Multicast 843

Multicast Optimization 843
Configuring IP Multicast VLAN for WLAN (GUI) 844
Configuring IP Multicast VLAN for WLAN 844
Verifying the Multicast VLAN Configuration 845
Multicast Filtering 846
Information About Multicast Filtering 846
Configuring Multicast Filtering 847
Verifying Multicast Filtering 847

CHAPTER 77 **Map-Server Per-Site Support** 849
Information About Map Server Per Site Support 849
Configuring the Default Map Server (GUI) 850
Configuring the Default Map Server (CLI) 850
Configuring a Map Server Per Site (GUI) 851
Configuring a Map Server Per Site (CLI) 851
Creating a Map Server for Each VNID (GUI) 852
Creating a Map Server for Each VNID 852
Creating a Fabric Profile and Associating a Tag and VNID (GUI) 853
Creating a Fabric Profile and Associating a Tag and VNID (CLI) 853
Verifying the Map Server Configuration 854

CHAPTER 78 **Volume Metering** 857
Volume Metering 857
Configuring Volume Metering 857

CHAPTER 79 **Enabling Syslog Messages in Access Points and Controller for Syslog Server** 859
Information About Enabling Syslog Messages in Access Points and Controller for Syslog Server 859
Configuring Syslog Server for an AP Profile 861
Configuring Syslog Server for the Controller (GUI) 862
Configuring Syslog Server for the Controller 863
Information About Syslog Support for Client State Change 864
Configuring Syslog Support for Client State Change (CLI) 865
Sample Syslogs 865
Verifying Syslog Server Configurations 866

CHAPTER 80 **Login Banner** 871

Information About Login Banner 871

Configuring a Login Banner (GUI) 871

Configuring a Login Banner 872

CHAPTER 81 **Wi-Fi Alliance Agile Multiband** 873

Introduction to Wi-Fi Alliance Agile Multiband 873

Limitations of MBO 875

Configuring MBO on a WLAN 875

Verifying MBO Configuration 876

CHAPTER 82 **SNMP Traps** 879

Information About Configuring SNMP Traps 879

Configuring SNMP Traps (GUI) 880

Enabling Access Points Traps (CLI) 880

Enabling Wireless Client Traps (CLI) 881

Enabling Mesh Traps (CLI) 881

Enabling RF Traps (CLI) 882

Enabling Rogue, Mobility, RRM, and General Traps (CLI) 882

Verifying SNMP Wireless Traps 883

CHAPTER 83 **Disabling Clients with Random MAC Address** 885

Information About Disabling Clients with Random MAC Addresses 885

Configuring Random MAC Address Deny (CLI) 885

Verifying Denial of Clients with a Random MAC Address 886

CHAPTER 84 **Dataplane Packet Logging** 889

Information About Dataplane Packet Logging 889

Enabling or Disabling Debug Level (CLI) 890

Enabling Packet Logging in Global and Filtered Buffer in Ingress Path (CLI) 890

Enabling Packet Logging in Global and Filtered Buffer in Punt-Inject Path (CLI) 891

Verifying Dataplane Packet Logging 892

Clearing Logs and Conditions in Global and Filtered Trace Buffers 893

CHAPTER 85 **Streaming Telemetry** 895

Information About Streaming Telemetry 895

Gather Points 895

Subscription 896

Transport 897

Scale Considerations 897

Session 897

gNMI Dial-In-Mode 897

gRPC- Dial-Out-Mode 898

Configuring Telemetry on a Cisco Catalyst 9800 Series Wireless Controller 898

Enabling gNXI in Insecure Mode (CLI) 898

Enabling gNXI in Secure Mode (CLI) 899

Verifying the Status of a Telemetry Subscription on a Cisco Catalyst 9800 Series Wireless Controller 901

Managing Configured Subscriptions on a Cisco Catalyst 9800 Series Wireless Controller 901

Zero Trust Telemetry 902

Define a Protocol 903

Define a Named Receiver 903

Configure Telemetry Subscription 904

On-Change Telemetry Support 905

Supported XPaths for On-Change Subscription 905

Troubleshooting Telemetry Support 909

Cisco Catalyst Center Client Event and SSID Telemetry Filter 911

Feature History for Cisco Catalyst Center Client Event and SSID Telemetry Filter 911

Information About Cisco Catalyst Center Client Event and SSID Telemetry Filter 912

Restrictions for Cisco Catalyst Center Client Event and SSID Telemetry Filter 913

Supported Workflow for Cisco Catalyst Center Client Event and SSID Telemetry Filter 913

Enabling iCAP Filtering in APs (CLI) 913

Disabling Client Telemetry Data for a WLAN (YANG) 914

Verifying Client Telemetry Data for a WLAN 914

CHAPTER 86 **Application Performance Monitoring** 915

Feature History for Application Performance Monitoring 915
Information About Application Performance Monitoring 915
Restrictions for Application Performance Monitoring 916
Workflow 916
Create a Flow Monitor 916
Create a Wireless WLAN Profile Policy 917
Create a Policy Tag 919
Attach the Policy Profile to an AP 919
Verify Application Performance Monitoring 920

CHAPTER 87 **Wireless Clients Threshold Warning** 921
Information About Wireless Clients Threshold Warning 921
Configuring a Warning Period 921
Configuring Client Threshold 922

PART VII **Security** 923

CHAPTER 88 **MAC Filtering** 925
MAC Filtering 925
MAC Filtering Configuration Guidelines 925
Configuring MAC Filtering for Local Authentication (CLI) 927
Configuring MAC Filtering (GUI) 928
Configuring MAB for External Authentication (CLI) 928

CHAPTER 89 **Web-Based Authentication** 931
Local Web Authentication Overview 931
Device Roles 933
Authentication Process 934
Local Web Authentication Banner 935
Customized Local Web Authentication 937
Guidelines 938
Redirection URL for Successful Login Guidelines 939
How to Configure Local Web Authentication 939
Configuring Default Local Web Authentication 939

Information About the AAA Wizard 940
Configuring AAA Authentication (GUI) 944
Configuring AAA Authentication (CLI) 944
Configuring the HTTP/HTTPS Server (GUI) 946
Configuring the HTTP Server (CLI) 946
Allowing Special Characters for Serial Port 947
Allowing Special Characters for VTY Port 948
Configuring HTTP and HTTPS Requests for Web Authentication 949
Information About Configuring HTTP and HTTPS Requests for Web Authentication 949
Guidelines and Limitations 951
Configuring HTTP and HTTPS Requests for Web Authentication (CLI) 951
Creating a Parameter Map (GUI) 952
Creating Parameter Maps 952
Configuring Local Web Authentication (GUI) 952
Configuring the Internal Local Web Authentication (CLI) 953
Configuring the Customized Local Web Authentication (CLI) 954
Configuring the External Local Web Authentication (CLI) 955
Configuring the Web Authentication WLANs 957
Configuring Pre-Auth Web Authentication ACL (GUI) 958
Configuring Pre-Auth Web Authentication ACL (CLI) 958
Configuring the Maximum Web Authentication Request Retries 960
Configuring a Local Banner in Web Authentication Page (GUI) 960
Configuring a Local Banner in Web Authentication Page (CLI) 961
Configuring Type WebAuth, Consent, or Both 961
Configuring Preauthentication ACL 962
Configuring TrustPoint for Local Web Authentication 963
Configuration Examples for Local Web Authentication 963
Example: Obtaining Web Authentication Certificate 963
Example: Displaying a Web Authentication Certificate 965
Example: Choosing the Default Web Authentication Login Page 965
Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server 966
Example: Choosing a Customized Web Authentication Login Page from an IPv6 External Web Server 966

Example: Assigning Login, Login Failure, and Logout Pages per WLAN 967
Example: Configuring Preauthentication ACL 967
Example: Configuring Webpassthrough 967
Verifying Web Authentication Type 968
External Web Authentication (EWA) 969
Configuring EWA with Single WebAuth Server Address and Default Ports (80/443) (CLI) 969
Configuring EWA with Multiple Web Servers and/or Ports Different than Default (80/443) 971
Configuring Wired Guest EWA with Multiple Web Servers and/or Ports Different than Default (80/443) 973
Authentication for Sleeping Clients 974
Information About Authenticating Sleeping Clients 974
Restrictions on Authenticating Sleeping Clients 974
Configuring Authentication for Sleeping Clients (GUI) 975
Configuring Authentication for Sleeping Clients (CLI) 975
Sleeping Clients with Multiple Authentications 976
Mobility Support for Sleeping Clients 976
Supported Combinations of Multiple Authentications 976
Configuring Sleeping Clients with Multiple Authentications 977
Configuring WLAN for Dot1x and Local Web Authentication 977
Configuring a WLAN for MAC Authentication Bypass and Local Web Authentication 978
Configuring a WLAN for Local Web Authentication and MAC Filtering 979
Configuring a PSK + LWA in a WLAN 980
Configuring a Sleeping Client 981
Verifying a Sleeping Client Configuration 982
Multi Authentication Combination with 802.1X Authentication and Local Web Authentication 982
Feature History for Multiauthentication Combination of 802.1X and Local Web Authentication 982
Information About Multiauthentication Combination with 802.1X Authentication and Local Web Authentication 982
Limitations for Multi Authentication Combination of 802.1X and Local Web Authentication 983
Enabling the Multiauthentication Combination of 802.1X Authentication and Local Web Authentication (CLI) 983
Verifying Multiauthentication Combination with 802.1X Authentication and Local Web Authentication 984

CHAPTER 90 **Central Web Authentication** 985

Information About Central Web Authentication 985
Prerequisites for Central Web Authentication 986
How to Configure ISE 986
Creating an Authorization Profile 986
Creating an Authentication Rule 987
Creating an Authorization Rule 987
How to Configure Central Web Authentication on the Controller 988
Configuring WLAN (GUI) 988
Configuring WLAN (CLI) 989
Configuring Policy Profile (CLI) 991
Configuring a Policy Profile (GUI) 992
Creating Redirect ACL 993
Configuring AAA for Central Web Authentication 994
Configuring Redirect ACL in Flex Profile (GUI) 994
Configuring Redirect ACL in Flex Profile (CLI) 995
Troubleshooting Central Web Authentication 996
Authentication for Sleeping Clients 996
Information About Authenticating Sleeping Clients 996
Restrictions on Authenticating Sleeping Clients 997
Configuring Authentication for Sleeping Clients (GUI) 997
Configuring Authentication for Sleeping Clients (CLI) 998
Sleeping Clients with Multiple Authentications 998
Mobility Support for Sleeping Clients 998
Supported Combinations of Multiple Authentications 998
Configuring Sleeping Clients with Multiple Authentications 999
Configuring WLAN for Dot1x and Local Web Authentication 999
Configuring a WLAN for MAC Authentication Bypass and Local Web Authentication 1000
Configuring a WLAN for Local Web Authentication and MAC Filtering 1001
Configuring a PSK + LWA in a WLAN 1002
Configuring a Sleeping Client 1003
Verifying a Sleeping Client Configuration 1004

CHAPTER 91 **Private Shared Key** 1005
Information About Private Preshared Key 1005

Configuring a PSK in a WLAN (CLI) 1006
Configuring a PSK in a WLAN (GUI) 1007
Applying a Policy Profile to a WLAN (GUI) 1008
Applying a Policy Profile to a WLAN (CLI) 1008
Verifying a Private PSK 1009

CHAPTER 92 Multi-Preshared Key 1013
Information About Multi-Preshared Key 1013
Restrictions on Multi-PSK 1014
Configuring Multi-Preshared Key (GUI) 1014
Configuring Multi-Preshared Key (CLI) 1017
Verifying Multi-PSK Configurations 1018

CHAPTER 93 Multiple Authentications for a Client 1021
Information About Multiple Authentications for a Client 1021
Information About Supported Combination of Authentications for a Client 1021
Jumbo Frame Support for RADIUS Packets 1022
Combination of Authentications on MAC Failure Not Supported on a Client 1023
Configuring Multiple Authentications for a Client 1023
Configuring WLAN for 802.1X and Local Web Authentication (GUI) 1023
Configuring WLAN for 802.1X and Local Web Authentication (CLI) 1023
Configuring WLAN for Preshared Key (PSK) and Local Web Authentication (GUI) 1025
Configuring WLAN for Preshared Key (PSK) and Local Web Authentication 1025
Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication (GUI) 1027
Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication 1027
Configuring WLAN 1027
Applying Policy Profile to a WLAN 1028
Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Pre-Shared Key (CLI) 1029
Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with OWE (CLI) 1031
Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Secure Agile Exchange (CLI) 1033
Configuring 802.1x and Central Web Authentication on Controller (CLIs) 1034

Creating AAA Authentication 1034
Configuring AAA Server for External Authentication 1035
Configuring AAA for Authentication 1036
Configuring Accounting Identity List 1037
Configuring AAA for Central Web Authentication 1037
Defining an Access Control List for Radius Server 1038
Configuration Example to Define an Access Control List for Radius Server 1038
Configuring WLAN 1039
Configuring Policy Profile 1039
Mapping WLAN and Policy Profile to Policy Tag 1040
Configuring ISE for Central Web Authentication with Dot1x (GUI) 1041
Defining Guest Portal 1041
Defining Authorization Profile for a Client 1041
Defining Authentication Rule 1041
Defining Authorization Rule 1042
Creating Rules to Match Guest Flow Condition 1042
Verifying Multiple Authentication Configurations 1043

CHAPTER 94 **Wi-Fi Protected Access 3** 1047
Simultaneous Authentication of Equals 1047
Opportunistic Wireless Encryption 1048
Hash-to-Element (H2E) 1048
YANG (RPC model) 1049
Transition Disable 1051
WPA3 SAE iPSK 1051
Configuring SAE (WPA3+WPA2 Mixed Mode) 1051
Configuring WPA3 Enterprise (GUI) 1053
Configuring WPA3 Enterprise 1053
Configuring the WPA3 OWE 1055
Configuring WPA3 OWE Transition Mode (GUI) 1056
Configuring WPA3 OWE Transition Mode 1056
Configuring WPA3 SAE (GUI) 1058
Configuring WPA3 SAE 1058
Configuring WPA3 SAE iPSK (CLI) 1060

Configuring a WPA3 SAE iPSK WLAN Profile (CLI) 1060
Configuring a Policy Profile (CLI) 1062
Configuring a Passphrase in a Client Authorization Policy in the RADIUS Server(GUI) 1062
Configuring WPA3 SAE H2E (GUI) 1063
Configuring WPA3 SAE H2E 1063
Configuring WPA3 WLAN for Transition Disable 1065
Configuring Anti-Clogging and SAE Retransmission (GUI) 1066
Configuring Anti-Clogging and SAE Retransmission 1066
Verifying WPA3 SAE and OWE 1067
Verifying WPA3 SAE H2E Support in WLAN 1071
Verifying WPA3 Transition Disable in WLAN 1076

CHAPTER 95 **IP Source Guard** 1081
Information About IP Source Guard 1081
Configuring IP Source Guard (GUI) 1081
Configuring IP Source Guard 1082

CHAPTER 96 **802.11w** 1083
Information About 802.11w 1083
Prerequisites for 802.11w 1086
Restrictions for 802.11w 1086
How to Configure 802.11w 1087
Configuring 802.11w (GUI) 1087
Configuring 802.11w (CLI) 1087
Disabling 802.11w 1088
Monitoring 802.11w 1089

CHAPTER 97 **Management Frame Protection** 1091
Information About Management Frame Protection 1091
Restrictions for Management Frame Protection 1092
Configuring Management Frame Protection (CLI) 1093
Verifying Management Frame Protection Settings 1093

CHAPTER 98 **IPv4 ACLs** 1095

Information about Network Security with ACLs 1095
ACL Overview 1095
Access Control Entries 1095
ACL Supported Types 1096
Supported ACLs 1096
ACL Precedence 1096
Port ACLs 1096
Router ACLs 1097
ACEs and Fragmented and Unfragmented Traffic 1098
ACEs and Fragmented and Unfragmented Traffic Examples 1098
Standard and Extended IPv4 ACLs 1099
IPv4 ACL Switch Unsupported Features 1099
Access List Numbers 1099
Numbered Standard IPv4 ACLs 1100
Numbered Extended IPv4 ACLs 1101
Named IPv4 ACLs 1101
ACL Logging 1102
Hardware and Software Treatment of IP ACLs 1102
IPv4 ACL Interface Considerations 1103
Restrictions for Configuring IPv4 Access Control Lists 1103
How to Configure ACLs 1104
Configuring IPv4 ACLs (GUI) 1104
Configuring IPv4 ACLs 1104
Creating a Numbered Standard ACL (GUI) 1105
Creating a Numbered Standard ACL (CLI) 1105
Creating a Numbered Extended ACL (GUI) 1107
Creating a Numbered Extended ACL (CLI) 1107
Creating Named Standard ACLs (GUI) 1111
Creating Named Standard ACLs 1111
Creating Extended Named ACLs (GUI) 1113
Creating Extended Named ACLs 1113
Applying an IPv4 ACL to an Interface (GUI) 1115
Applying an IPv4 ACL to an Interface (CLI) 1115
Applying ACL to Policy Profile (GUI) 1116

Applying ACL to Policy Profile 1116
Configuration Examples for ACLs 1117
Examples: Including Comments in ACLs 1117
Examples: Applying an IPv4 ACL to a Policy Profile in a Wireless Environment 1117
IPv4 ACL Configuration Examples 1118
ACLs in a Small Networked Office 1118
Examples: ACLs in a Small Networked Office 1119
Example: Numbered ACLs 1119
Examples: Extended ACLs 1120
Examples: Named ACLs 1120
Monitoring IPv4 ACLs 1121

CHAPTER 99 **Downloadable ACL** 1123
Feature History for Downloadable ACL 1123
Information About Downloadable ACL 1124
Scale Considerations for Downloadable ACL 1124
Guidelines and Restrictions for Downloadable ACL 1124
Configuring dACL Name and Definition in Cisco ISE 1125
Configuring dACL in a Controller (CLI) 1125
Configuring Explicit Authorization Server List (CLI) 1126
Verifying dACL Configuration 1127

CHAPTER 100 **DNS-Based Access Control Lists** 1129
Information About DNS-Based Access Control Lists 1129
Defining ACLs 1130
Applying ACLs 1131
Types of URL Filters 1131
Restrictions on DNS-Based Access Control Lists 1132
Flex Mode 1133
Defining URL Filter List 1133
Applying URL Filter List to Flex Profile 1134
Configuring ISE for Central Web Authentication (GUI) 1134
Local Mode 1135
Defining URL Filter List 1135

Applying URL Filter List to Policy Profile (GUI) 1136
Applying URL Filter List to Policy Profile 1137
Configuring ISE for Central Web Authentication 1137
Creating Authorization Profiles 1137
Mapping Authorization Profiles to Authentication Rule 1138
Mapping Authorization Profiles to Authorization Rule 1138
Viewing DNS-Based Access Control Lists 1139
Configuration Examples for DNS-Based Access Control Lists 1139
Verifying DNS Snoop Agent (DSA) 1140
Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL 1141
Enabling Pre-Authentication ACL for LWA and EWA (GUI) 1142
Enabling Pre-Authentication ACL for LWA and EWA 1143
Enabling Post-Authentication ACL for LWA and EWA (GUI) 1144
Enabling Post-Authentication ACL for LWA and EWA 1145
Enabling DNS ACL for LWA and EWA (GUI) 1145
Enabling DNS ACL for LWA and EWA 1145
Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL 1146

CHAPTER 101 **Allowed List of Specific URLs** 1147
Allowed List of Specific URLs 1147
Adding URL to Allowed List 1147
Verifying URLs on the Allowed List 1149

CHAPTER 102 **Cisco Umbrella WLAN** 1151
Information About Cisco Umbrella WLAN 1151
Registering Controller to Cisco Umbrella Account 1152
Configuring Cisco Umbrella WLAN 1153
Importing CA Certificate to the Trust Pool 1153
Creating a Local Domain RegEx Parameter Map 1155
Configuring Parameter Map Name in WLAN (GUI) 1155
Configuring the Umbrella Parameter Map 1156
Enabling or Disabling DNScrypt (GUI) 1156
Enabling or Disabling DNScrypt 1157
Configuring Timeout for UDP Sessions 1157

Configuring Parameter Map Name in WLAN (GUI) 1158
Configuring Parameter Map Name in WLAN 1158
Configuring the Umbrella Flex Profile 1159
Configuring the Umbrella Flex Profile (GUI) 1159
Configuring Umbrella Flex Parameters 1160
Configuring the Umbrella Flex Policy Profile (GUI) 1160
Verifying the Cisco Umbrella Configuration 1161

CHAPTER 103 RADIUS Server Load Balancing 1163
Information About RADIUS Server Load Balancing 1163
Prerequisites for RADIUS Server Load Balancing 1165
Restrictions for RADIUS Server Load Balancing 1165
Enabling Load Balancing for a Named RADIUS Server Group (CLI) 1165

CHAPTER 104 AAA Dead-Server Detection 1167
Information About AAA Dead-Server Detection 1167
Prerequisites for AAA Dead-Server Detection 1168
Restrictions for AAA Dead-Server Detection 1168
Configuring AAA Dead-Server Detection (CLI) 1168
Verifying AAA Dead-Server Detection 1169

CHAPTER 105 ISE Simplification and Enhancements 1171
Utilities for Configuring Security 1171
Configuring Multiple Radius Servers 1172
Verifying AAA and Radius Server Configurations 1173
Configuring Captive Portal Bypassing for Local and Central Web Authentication 1173
Information About Captive Bypassing 1173
Configuring Captive Bypassing for WLAN in LWA and CWA (GUI) 1174
Configuring Captive Bypassing for WLAN in LWA and CWA (CLI) 1175
Sending DHCP Options 55 and 77 to ISE 1176
Information about DHCP Option 55 and 77 1176
Configuration to Send DHCP Options 55 and 77 to ISE (GUI) 1176
Configuration to Send DHCP Options 55 and 77 to ISE (CLI) 1176
Configuring EAP Request Timeout (GUI) 1177

Configuring EAP Request Timeout 1178
Configuring EAP Request Timeout in Wireless Security (CLI) 1178
Captive Portal 1179
Captive Portal Configuration 1179
Configuring Captive Portal (GUI) 1179
Configuring Captive Portal 1180
Captive Portal Configuration - Example 1182

CHAPTER 106 RADIUS DTLS 1185
Information About RADIUS DTLS 1185
Prerequisites 1187
Configuring RADIUS DTLS Server 1187
Configuring RADIUS DTLS Connection Timeout 1188
Configuring RADIUS DTLS Idle Timeout 1188
Configuring Source Interface for RADIUS DTLS Server 1189
Configuring RADIUS DTLS Port Number 1190
Configuring RADIUS DTLS Connection Retries 1190
Configuring RADIUS DTLS Trustpoint 1191
Configuring RADIUS DTLS Match-Server-Identity 1192
Configuring DTLS Dynamic Author 1192
Enabling DTLS for Client 1193
Configuring Client Trustpoint for DTLS 1193
Configuring DTLS Idle Timeout 1194
Configuring Server Trustpoint for DTLS 1195
Verifying the RADIUS DTLS Server Configuration 1195
Clearing RADIUS DTLS Specific Statistics 1195

CHAPTER 107 Policy Enforcement and Usage Monitoring 1197
Policy Enforcement and Usage Monitoring 1197
Configuring Policy Enforcement and Enabling Change-of-Authorization (CLI) 1197
Example: Configuring Policy Enforcement and Usage Monitoring 1198
Verifying Policy Usage and Enforcement 1199

CHAPTER 108 Local Extensible Authentication Protocol 1201

Information About Local EAP 1201
Restrictions for Local EAP 1202
Configuring Local EAP Profile (CLI) 1202
Configuring Local EAP profile (GUI) 1203
Configuring AAA Authentication (GUI) 1203
Configuring AAA Authorization Method (GUI) 1203
Configuring AAA Authorization Method (CLI) 1204
Configuring Local Advanced Methods (GUI) 1205
Configuring WLAN (GUI) 1205
Configuring WLAN (CLI) 1206
Creating a User Account (CLI) 1206
Attaching a Policy Profile to a WLAN Interface (GUI) 1207
Deploy Policy Tag to Access Points (GUI) 1208

CHAPTER 109 **Local EAP Ciphersuite** 1209
Information About Local EAP Ciphersuite 1209
Restrictions for Local EAP Ciphersuite 1210
Configuring Local EAP Ciphersuite (CLI) 1211

CHAPTER 110 **Authentication and Authorization Between Multiple RADIUS Servers** 1213
Information About Authentication and Authorization Between Multiple RADIUS Servers 1213
Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers 1214
Configuring Explicit Authentication and Authorization Server List (GUI) 1214
Configuring Explicit Authentication Server List (GUI) 1215
Configuring Explicit Authentication Server List (CLI) 1215
Configuring Explicit Authorization Server List (GUI) 1216
Configuring Explicit Authorization Server List (CLI) 1217
Configuring Authentication and Authorization List for 802.1X Security (GUI) 1218
Configuring Authentication and Authorization List for 802.1X Security 1218
Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers 1219
Configuring Authentication and Authorization List for Web Authentication (GUI) 1219
Configuring Authentication and Authorization List for Web Authentication 1220
Verifying Split Authentication and Authorization Configuration 1221
Configuration Examples 1222

CHAPTER 111 **CUI Information in RADIUS Accounting** 1223

CUI Information in RADIUS Accounting Request 1223

Adding CUI Information in a RADIUS Accounting Request 1224

Verifying CUI Information in a RADIUS Accounting Request 1224

CHAPTER 112 **Secure LDAP** 1225

Information About SLDAP 1225

Prerequisite for Configuring SLDAP 1227

Restrictions for Configuring SLDAP 1227

Configuring SLDAP 1227

Configuring an AAA Server Group (GUI) 1228

Configuring a AAA Server Group 1229

Configuring Search and Bind Operations for an Authentication Request 1230

Configuring a Dynamic Attribute Map on an SLDAP Server 1231

Verifying the SLDAP Configuration 1231

CHAPTER 113 **Network Access Server Identifier** 1233

Information About Network Access Server Identifier 1233

Creating a NAS ID Policy(GUI) 1234

Creating a NAS ID Policy 1234

Attaching a Policy to a Tag (GUI) 1235

Attaching a Policy to a Tag (CLI) 1235

Verifying the NAS ID Configuration 1236

CHAPTER 114 **Locally Significant Certificates** 1239

Information About Locally Significant Certificates 1239

Certificate Provisioning in Controllers 1240

Device Certificate Enrollment Operation 1240

Certificate Provisioning on Lightweight Access Point 1240

Restrictions for Locally Significant Certificates 1241

Provisioning Locally Significant Certificates 1242

Configuring RSA Key for PKI Trustpoint 1242

Configuring PKI Trustpoint Parameters 1242

Authenticating and Enrolling a PKI Trustpoint (GUI) 1243
Authenticating and Enrolling the PKI Trustpoint with CA Server (CLI) 1244
Configuring AP Join Attempts with LSC Certificate (GUI) 1245
Configuring AP Join Attempts with LSC Certificate (CLI) 1246
Configuring Subject-Name Parameters in LSC Certificate 1246
Configuring Key Size for LSC Certificate 1247
Configuring Trustpoint for LSC Provisioning on an Access Point 1247
Configuring an AP LSC Provision List (GUI) 1247
Configuring an AP LSC Provision List (CLI) 1248
Configuring LSC Provisioning for all the APs (GUI) 1249
Configuring LSC Provisioning for All APs (CLI) 1250
Configuring LSC Provisioning for the APs in the Provision List 1250
Importing a CA Certificate to the Trustpool (GUI) 1250
Importing a CA Certificate to the Trustpool (CLI) 1251
Cleaning the CA Certificates Imported in Trustpool (GUI) 1252
Cleaning CA Certificates Imported in Trustpool (CLI) 1252
Creating a New Trustpoint Dedicated to a Single CA Certificate 1252
Verifying LSC Configuration 1253
Configuring Management Trustpoint to LSC (GUI) 1254
Configuring Management Trustpoint to LSC (CLI) 1254
Information About MIC and LSC Access Points Joining the Controller 1255
Overview of Support for MIC and LSC Access Points Joining the Controller 1255
Recommendations and Limitations 1255
Configuration Workflow 1255
Configuring LSC on the Controller (CLI) 1255
Enabling the AP Certificate Policy on the APs (CLI) 1256
Configuring the AP Policy Certificate (GUI) 1257
Configuring the Allowed List of APs to Join the Controller (CLI) 1258
Verifying the Configuration Status 1258
LSC Fallback Access Points 1259
Information About LSC Fallback APs 1259
Troubleshooting LSC Fallback State 1259
Recovery Steps 1260
Configuring Controller Self-Signed Certificate for Wireless AP Join 1260

Use Cases 1260
Prerequisites 1261
Configuring Clock Calendar (CLI) 1261
Enabling HTTP Server (CLI) 1262
Configuring CA Server (CLI) 1262
Configuring Trustpoint (CLI) 1264
Authenticating and Enrolling the PKI TrustPoint with CA Server (CLI) 1265
Tagging Wireless Management TrustPoint Name (CLI) 1266
Verifying Controller Certificates for Wireless AP Join 1266

CHAPTER 115 Certificate Management 1269
About Public Key Infrastructure Management (GUI) 1269
Authenticating and Enrolling a PKI Trustpoint (GUI) 1269
Generating an AP Self-Signed Certificate (GUI) 1270
Adding the Certificate Authority Server (GUI) 1270
Adding an RSA or EC Key for PKI Trustpoint (GUI) 1271
Adding and Managing Certificates 1271
1272

CHAPTER 116 Controller Self-Signed Certificate for Wireless AP Join 1273
Use Cases 1273
Prerequisites 1274
Configuring Clock Calendar (CLI) 1274
Enabling HTTP Server (CLI) 1275
Configuring CA Server (CLI) 1275
Configuring Trustpoint (CLI) 1277
Authenticating and Enrolling the PKI TrustPoint with CA Server (CLI) 1278
Tagging Wireless Management TrustPoint Name (CLI) 1279
Verifying Controller Certificates for Wireless AP Join 1279

CHAPTER 117 Managing Rogue Devices 1281
Rogue Detection 1281
Rogue Devices 1281
Information About Rogue Containment (Protected Management Frames (PMF) Enabled) 1283

AP Impersonation Detection 1284
Configuring Rogue Detection (GUI) 1284
Configuring Rogue Detection (CLI) 1285
Configuring RSSI Deviation Notification Threshold for Rogue APs (CLI) 1286
Configuring Management Frame Protection (GUI) 1286
Configuring Management Frame Protection (CLI) 1287
Enabling Access Point Authentication 1287
Verifying Management Frame Protection 1288
Verifying Rogue Events 1288
Verifying Rogue Detection 1289
Examples: Rogue Detection Configuration 1290
Configuring Rogue Policies (GUI) 1291
Configuring Rogue Policies (CLI) 1291
Rogue Detection Security Level 1293
Setting Rogue Detection Security-level 1294
Wireless Service Assurance Rogue Events 1295
Monitoring Wireless Service Assurance Rogue Events 1296
Rogue Full Scale Quotas and Priorities 1296
Feature History for Rogue Full Scale Quotas and Priorities 1296
Rogue AP Scale Modes Per Class 1297
Configuring Rogue AP Scale (CLI) 1298
Verifying Rogue Scale Details 1299

CHAPTER 118 **Classifying Rogue Access Points** 1301
Information About Classifying Rogue Access Points 1301
Guidelines and Restrictions for Classifying Rogue Access Points 1303
How to Classify Rogue Access Points 1303
Classifying Rogue Access Points and Clients Manually (GUI) 1303
Classifying Rogue Access Points and Clients Manually (CLI) 1304
Configuring Rogue Classification Rules (GUI) 1305
Configuring Rogue Classification Rules (CLI) 1306
Monitoring Rogue Classification Rules 1309
Examples: Classifying Rogue Access Points 1309

CHAPTER 119 Advanced WIPS 1311

Feature History for Advanced WIPS 1311

Information About Advanced WIPS 1312

Guidelines and Restrictions 1314

Enabling Advanced WIPS 1315

Syslog Support for Advanced WIPS 1315

Advanced WIPS Solution Components 1316

Supported Modes and Platforms 1316

Enabling Advanced WIPS(GUI) 1317

Enabling Advanced WIPS (CLI) 1317

Configuring Syslog Threshold for Advanced WIPS (CLI) 1318

Viewing Advanced WIPS Alarms (GUI) 1318

Verifying Advanced WIPS 1319

Verifying Syslog Configuration for Advanced WIPS 1320

CHAPTER 120 Cisco TrustSec 1321

Information about Cisco TrustSec 1321

Cisco TrustSec Features 1322

Security Group Access Control List 1323

Inline Tagging 1325

Policy Enforcement 1325

SGACL Support for Wireless Guest Access 1326

Enabling SGACL on the AP (GUI) 1326

Enabling SGACL on the AP 1327

Enabling SGACL Policy Enforcement Globally (CLI) 1328

Enabling SGACL Policy Enforcement Per Interface (CLI) 1329

Manually Configure a Device SGT (CLI) 1329

Configuring SGACL, Inline Tagging, and SGT in Local Mode (GUI) 1330

Configuring SGACL, Inline Tagging, and SGT in Local Mode 1330

Configuring ISE for TrustSec 1331

Verifying Cisco TrustSec Configuration 1333

CHAPTER 121 SGT Inline Tagging and SXPv4 1335

Introduction to SGT Inline Tagging on AP and SXPv4 1335
Creating an SXP Profile 1335
Configuring SGT Inline Tagging on Access Points 1336
Configuring an SXP Connection (GUI) 1336
Configuring an SXP Connection 1337
Verifying SGT Push to Access Points 1338

CHAPTER 122 **Multiple Cipher Support** 1341
Default Ciphersuites Supported for CAPWAP-DTLS 1341
Configuring Multiple Ciphersuites 1342
Setting Server Preference 1343
Verifying Operational Ciphersuites and Priority 1343

CHAPTER 123 **Configuring Secure Shell** 1345
Information About Configuring Secure Shell 1345
SSH and Device Access 1345
SSH Servers, Integrated Clients, and Supported Versions 1345
SSH Configuration Guidelines 1346
Secure Copy Protocol Overview 1346
Secure Copy Protocol 1347
SFTP Support 1347
Prerequisites for Configuring Secure Shell 1347
Restrictions for Configuring Secure Shell 1348
How to Configure SSH 1349
Setting Up the Device to Run SSH 1349
Configuring the SSH Server 1350
Monitoring the SSH Configuration and Status 1351

CHAPTER 124 **Encrypted Traffic Analytics** 1353
Information About Encrypted Traffic Analytics 1353
Exporting Records to IPv4 Flow Export Destination 1354
Exporting Records to IPv6 Flow Export Destination 1355
Exporting Records to IPv4 and IPv6 Destination over IPFIX 1355
Allowed List of Traffic 1356

Configuring Source Interface for Record Export 1357
Configuring Source Interface for Record Export Without IPFIX 1358
Configuring ETA Flow Export Destination (GUI) 1359
Enabling In-Active Timer 1359
Enabling ETA on WLAN Policy Profile 1360
Attaching Policy Profile to VLAN (GUI) 1361
Attaching Policy Profile to VLAN 1361
Verifying ETA Configuration 1362

CHAPTER 125 **FIPS** 1367
FIPS 1367
Guidelines and Restrictions for FIPS 1368
FIPS Self-Tests 1368
Configuring FIPS 1369
Configuring FIPS in HA Setup 1370
Verifying FIPS Configuration 1371

CHAPTER 126 **Internet Protocol Security** 1373
Information about Internet Protocol Security 1373
Internet Key Exchange Version 1 Transform Sets 1374
Configure IPSec Using Internet Key Exchange Version 1 1375
Internet Key Exchange Version 2 Transform Sets 1377
Configure IPSec Using Internet Key Exchange Version 2 1378
IPsec Transforms and Lifetimes 1380
Use of X.509 With Internet Key Exchange Version 1381
For IKEv2 Commands 1382
IPsec Session Interruption and Recovery 1382
Example: Configure IPSec Using ISAKMP 1383
Verifying IPSec Traffic 1383
Example: Configure IPSec Using Internet Key Exchange Version 2 1384
Verifying IPSec With Internet Key Exchange Version 2 Traffic 1385

CHAPTER 127 **Transport Layer Security Tunnel Support** 1389
Information About Transport Layer Security Tunnel Support 1389

Configuring a Transport Layer Security Tunnel 1390
Verifying a Transport Layer Security Tunnel 1391

CHAPTER 128 Configuring RFC 5580 Location Attributes 1395
Feature History for RFC 5580 Location Attributes 1395
Information About RFC 5580 Location Attributes 1396
Information About Location-Capable Attribute 1398
Restriction for Configuring RFC 5580 Location Attributes 1398
Configuring Location Delivery Based on Out-of-Band Agreement (CLI) 1398
Configuring Location-Capable Attribute (CLI) 1399
Creating Location Attributes 1399
Configuring a Civic Profile (CLI) 1399
Configuring a Geo Profile (CLI) 1401
Configuring an Operator Name (CLI) 1402
Associating Location Attributes with User Location (CLI) 1403
Associating Location Attributes with the NAS Location (CLI) 1404
Verifying RFC 5580 Location Attribute Configuration 1405

CHAPTER 129 IP MAC Binding 1407
Information About IP MAC Binding 1407
Use Cases for No IP MAC Binding 1407
Disabling IP MAC Binding (CLI) 1408
Verifying IP MAC Binding 1408

CHAPTER 130 Disabling IP Learning in FlexConnect Mode 1409
Information About Disabling IP Learning in FlexConnect Mode 1409
Restrictions for Disabling IP Learning in FlexConnect Mode 1409
Disabling IP Learning in FlexConnect Mode (CLI) 1410
Verifying MAC Entries from Database 1410

CHAPTER 131 Disabling Device Tracking to Support NAC Devices 1411
Feature History for Disabling Device Tracking to Support NAC Devices 1411
Information About Disabling Device Tracking to Support NAC Devices 1411
Restrictions for Disabling Device Tracking to Support NAC Devices 1412

Disabling Device Tracking for Wireless Clients (CLI) 1412
Verifying ARP Broadcast 1413

PART VIII **Mobility** 1415

CHAPTER 132 **Mobility** 1417
Introduction to Mobility 1417
SDA Roaming 1420
Definitions of Mobility-related Terms 1421
Mobility Groups 1421
Guidelines and Restrictions 1422
Configuring Mobility (GUI) 1424
Configuring Mobility (CLI) 1425
Configuring Inter-Release Controller Mobility (GUI) 1427
Configuring Inter-Release Controller Mobility 1427
Verifying Mobility 1431

CHAPTER 133 **NAT Support on Mobility Groups** 1437
Information About NAT Support on Mobility Groups 1437
Restrictions for NAT Support on Mobility Groups 1438
Functionalities Supported on Mobility NAT 1438
Configuring a Mobility Peer 1439
Verifying NAT Support on Mobility Groups 1439

CHAPTER 134 **Static IP Client Mobility** 1441
Information About Static IP Client Mobility 1441
Restrictions 1441
Configuring Static IP Client Mobility (GUI) 1442
Configuring Static IP Client Mobility (CLI) 1442
Verifying Static IP Client Mobility 1443

CHAPTER 135 **Mobility Domain ID - Dot11i Roaming** 1445
Information about Mobility Domain ID - 802.11i Roaming 1445
Verifying Mobility Domain ID - 802.11i Roaming 1446

CHAPTER 136 **802.11r Support for Flex Local Authentication** 1447

Information About 802.11r Support for FlexConnect Local Authentication 1447

Support Guidelines 1447

Verifying 802.11r Support for Flex Local Authentication 1448

CHAPTER 137 **Opportunistic Key Caching** 1449

Information about Opportunistic Key Caching 1449

Enabling Opportunistic Key Caching 1450

Enabling Opportunistic Key Caching (GUI) 1450

Verifying Opportunistic Key Caching 1450

PART IX **High Availability** 1453

CHAPTER 138 **High Availability** 1455

Feature History for High Availability 1456

Information About High Availability 1457

Prerequisites for High Availability 1458

Restrictions on High Availability 1459

Configuring High Availability (CLI) 1460

Disabling High Availability 1461

Copying a WebAuth Tar Bundle to the Standby Controller 1462

System and Network Fault Handling 1464

Handling Recovery Mechanism 1469

Verifying High Availability Configurations 1470

Verifying AP or Client SSO Statistics 1470

Verifying High Availability 1472

High Availability Deployment for Application Centric Infrastructure (ACI) Network 1475

Information About Deploying ACI Network in Controller 1475

Prerequisite for Deploying the ACI Network in the Controller 1477

Disabling the Fast Switchover Notification Mechanism (CLI) 1477

Configuring Gratuitous ARP (GARP) Retransmit (CLI) 1478

Disabling Initial GARP (CLI) 1478

Configuring a Switchover 1479

Information About Redundancy Management Interface 1479
Configuring Redundancy Management Interface (GUI) 1484
Configuring Redundancy Management Interface (CLI) 1485
Configuring Gateway Monitoring (CLI) 1487
Configuring Gateway Monitoring Interval (CLI) 1487
Gateway Reachability Detection 1488
Information About Gateway Reachability Detection 1488
Configuration Workflow 1488
Migrating to RMI IPv6 1489
Monitoring the Health of the Standby Controller 1489
Monitoring the Health of Standby Parameters Using SNMP 1491
Standby Monitoring Using Standby RMI IP 1491
Standby Monitoring Using the Active Controller 1491
Standby IOS Linux Syslogs 1492
Standby Interface Status Using Active SNMP 1492
Monitoring the Health of Standby Controller Using Programmatic Interfaces 1493
Monitoring the Health of Standby Controller Using CLI 1493
Verifying the Gateway-Monitoring Configuration 1497
Verifying the RMI IPv4 Configuration 1497
Verifying the RMI IPv6 Configuration 1499
Verifying Redundancy Port Interface Configuration 1499
Information About Auto-Upgrade 1502
Use Cases 1502
Configuration Workflow 1502
Configuring Auto-Upgrade (CLI) 1503
Use Case for Link Layer Discovery Protocol (LLDP) 1503
Enabling LLDP (CLI) 1503
Enabling LLDP Timers (CLI) 1504
Enabling LLDP TLV-Select (CLI) 1504
Verifying LLDP 1505

PART X **Quality of Service** 1509

CHAPTER 139 **Quality of Service** 1511

Wireless QoS Overview 1511
Wireless QoS Targets 1512
SSID Policies 1512
Client Policies 1512
Supported QoS Features on Wireless Targets 1512
Wireless QoS Mobility 1513
Precious Metal Policies for Wireless QoS 1513
Prerequisites for Wireless QoS 1514
Restrictions for QoS on Wireless Targets 1514
Metal Policy Format 1515
Metal Policy Map 1515
Class Maps 1517
DSCP to UP Mapping for Downstream Traffic 1518
Auto QoS Policy Format 1519
Architecture for Voice, Video and Integrated Data (AVVID) 1521
How to apply Bi-Directional Rate Limiting 1522
Information about Bi-Directional Rate Limiting 1522
Prerequisites for Bi-Directional Rate Limiting 1523
Configure Metal Policy on SSID 1524
Configure Metal Policy on Client 1524
Configure Bi-Directional Rate Limiting for All Traffic 1525
Configure Bi-Directional Rate Limiting Based on Traffic Classification 1525
Apply Bi-Directional Rate Limiting Policy Map to Policy Profile 1527
Apply Metal Policy with Bi-Directional Rate Limiting 1528
How to apply Per Client Bi-Directional Rate Limiting 1529
Information About Per Client Bi-Directional Rate Limiting 1529
Prerequisites for Per Client Bi-Directional Rate Limiting 1530
Restrictions on Per Client Bi-Directional Rate Limiting 1530
Configuring Per Client Bi-Directional Rate Limiting (GUI) 1531
Verifying Per Client Bi-Directional Rate Limiting 1531
Configuring BDRL Using AAA Override 1531
Verifying Bi-Directional Rate-Limit 1532
How to Configure Wireless QoS 1534
Configuring a Policy Map with Class Map (GUI) 1534

Configuring a Class Map (CLI) 1535
Configuring Policy Profile to Apply QoS Policy (GUI) 1535
Configuring Policy Profile to Apply QoS Policy (CLI) 1536
Applying Policy Profile to Policy Tag (GUI) 1537
Applying Policy Profile to Policy Tag (CLI) 1537
Attaching Policy Tag to an AP 1538
Configuring Custom QoS Mapping 1538
Configuring DSCP-to-User Priority Mapping Exception 1539
Configuring Trust Upstream DSCP Value 1541

CHAPTER 140 **Wireless Auto-QoS** 1543
Information About Auto QoS 1543
How to Configure Wireless AutoQoS 1544
Configuring Wireless AutoQoS on Profile Policy 1544
Disabling Wireless AutoQoS 1545
Rollback AutoQoS Configuration (GUI) 1545
Rollback AutoQoS Configuration 1545
Clearing Wireless AutoQoS Policy Profile (GUI) 1546
Clearing Wireless AutoQoS Policy Profile 1546
Viewing AutoQoS on policy profile 1547

CHAPTER 141 **Native Profiling** 1549
Information About Native Profiling 1549
Creating a Class Map (GUI) 1550
Creating a Class Map (CLI) 1551
Creating a Service Template (GUI) 1553
Creating a Service Template (CLI) 1554
Creating a Parameter Map 1555
Creating a Policy Map (GUI) 1555
Creating a Policy Map (CLI) 1556
Configuring Native Profiling in Local Mode 1558
Verifying Native Profile Configuration 1558

CHAPTER 142 **Air Time Fairness** 1561

Information About Air Time Fairness 1561
Restrictions on Cisco Air Time Fairness 1563
Cisco Air Time Fairness (ATF) Use Cases 1564
Configuring Cisco Air Time Fairness (ATF) 1564
Configuring Cisco Air Time Fairness 1564
Creating a Cisco ATF Profile (GUI) 1564
Creating Cisco ATF Profile (CLI) 1565
Attaching Cisco ATF Profile to a Policy Profile (GUI) 1566
Attaching Cisco ATF Profile to a Policy Profile (CLI) 1566
Enabling ATF in the RF Profile (GUI) 1567
Enabling ATF in the RF Profile (CLI) 1567
Verifying Cisco ATF Configurations 1568
Verifying Cisco ATF Statistics 1568

CHAPTER 143 **IPv6 Non-AVC QoS Support** 1571
Information About IPv6 Non-AVC QoS Support 1571
Configuring IPv6 Non-AVC QoS 1571
Marking DSCP Values for an IPv6 Packet 1572
Dropping an IPv6 Packet with DSCP Values 1572
Policing IPv6 Traffic 1573
Verifying IPv6 Non-AVC QoS 1574

CHAPTER 144 **QoS Basic Service Set Load** 1575
Information About QoS Basic Set Service Load 1575
Configuring QBSS Load 1576
Configuring Wi-Fi Multimedia 1576
Enabling QoS Basic Set Service Load 1577
Verifying QoS Basic Set Service Load 1577

PART XI **IPv6** 1579

CHAPTER 145 **IPv6 Client IP Address Learning** 1581
Information About IPv6 Client Address Learning 1581
Address Assignment Using SLAAC 1581

Stateful DHCPv6 Address Assignment 1582
Router Solicitation 1583
Router Advertisement 1583
Neighbor Discovery 1583
Neighbor Discovery Suppression 1584
Router Advertisement Guard 1584
Router Advertisement Throttling 1585
Prerequisites for IPv6 Client Address Learning 1585
IPv6 Address Tracking for Wireless Clients 1585
Configuring Unknown Address Multicast Neighbor Solicitation Forwarding 1586
Configuring RA Throttle Policy (CLI) 1586
Applying RA Throttle Policy on VLAN (GUI) 1587
Applying RA Throttle Policy on a VLAN (CLI) 1588
Configuring IPv6 Interface on a Switch (GUI) 1588
Configuring IPv6 on Interface (CLI) 1589
Configuring DHCP Pool on Switch (GUI) 1590
Configuring DHCP Pool on Switch (CLI) 1590
Configuring Stateless Auto Address Configuration Without DHCP on Switch (CLI) 1591
Configuring Stateless Auto Address Configuration With DHCP on Switch 1593
Configuring Stateless Address Auto Configuration Without DHCP on Switch (CLI) 1594
Native IPv6 1595
Information About IPv6 1595
Configuring IPv6 Addressing 1596
Creating an AP Join Profile (GUI) 1597
Creating an AP Join Profile (CLI) 1598
Configuring the Primary and Backup Controller (GUI) 1598
Configuring Primary and Backup Controller (CLI) 1598
Verifying IPv6 Configuration 1599

CHAPTER 146 IPv6 ACL 1601
Information About IPv6 ACL 1601
Understanding IPv6 ACLs 1601
Types of ACL 1601
Per User IPv6 ACL 1601

Filter ID IPv6 ACL 1602
Prerequisites for Configuring IPv6 ACL 1602
Restrictions for Configuring IPv6 ACL 1602
Configuring IPv6 ACLs 1602
Default IPv6 ACL Configuration 1603
Interaction with Other Features and Switches 1603
How To Configure an IPv6 ACL 1603
Creating an IPv6 ACL (GUI) 1603
Creating an IPv6 ACL 1604
Creating WLAN IPv6 ACL (GUI) 1608
Creating WLAN IPv6 ACL 1608
Verifying IPv6 ACL 1608
Displaying IPv6 ACLs 1608
Configuration Examples for IPv6 ACL 1609
Example: Creating an IPv6 ACL 1609
Example: Applying an IPv6 ACL to a Policy Profile in a Wireless Environment 1609
Displaying IPv6 ACLs 1610
Example: Displaying IPv6 ACLs 1610
Example: Configuring RA Throttling 1611

CHAPTER 147 **IPv6 Client Mobility** 1613
Information About IPv6 Client Mobility 1613
Using Router Advertisement 1614
Router Advertisement Throttling 1614
IPv6 Address Learning 1615
Handling Multiple IP Addresses 1615
IPv6 Configuration 1615
Prerequisites for IPv6 Client Mobility 1615
Monitoring IPv6 Client Mobility 1616

CHAPTER 148 **IPv6 Support on Flex and Mesh** 1617
IPv6 Support on Flex + Mesh Deployment 1617
Configuring IPv6 Support for Flex + Mesh 1617
Configuring Preferred IP Address as IPv6 (GUI) 1618

Configuring Preferred IP Address as IPv6 1619
Verifying IPv6 on Flex+Mesh 1619

CHAPTER 149 IPv6 CAPWAP UDP Lite Support 1621
Information About UDP Lite 1621
Enabling UDP Lite Support 1621
Verifying UDP Lite Support Configuration 1622

CHAPTER 150 Neighbor Discovery Proxy 1623
Information About Neighbor Discovery 1623
Configure Neighbor Discovery Proxy (CLI) 1623
Configure Duplicate Address Detection Proxy (CLI) 1624

CHAPTER 151 Address Resolution Protocol Proxy 1627
Information About Address Resolution Protocol 1627
Configure Address Resolution Protocol Proxy (CLI) 1627

CHAPTER 152 IPv6 Ready Certification 1629
Feature History for IPv6-Ready Certification 1629
IPv6 Ready Certification 1629
Configuring IPv6 Route Information 1630
Verifying IPv6 Route Information 1630

PART XII CleanAir 1631

CHAPTER 153 Cisco CleanAir 1633
Feature History for CleanAir 1633
Information About Cisco CleanAir 1633
Cisco CleanAir-Related Terms 1634
Cisco CleanAir Components 1634
Interference Types that Cisco CleanAir can Detect 1636
EDRRM and AQR Update Mode 1637
Prerequisites for CleanAir 1637
Restrictions for CleanAir 1637

How to Configure CleanAir 1638
Enabling CleanAir for the 2.4-GHz Band (GUI) 1638
Enabling CleanAir for the 2.4-GHz Band (CLI) 1638
Configuring Interference Reporting for a 2.4-GHz Device (GUI) 1638
Configuring Interference Reporting for a 2.4-GHz Device (CLI) 1639
Enabling CleanAir for the 5-GHz Band (GUI) 1641
Enabling CleanAir for the 5-GHz Band (CLI) 1641
Configuring Interference Reporting for a 5-GHz Device (GUI) 1642
Configuring Interference Reporting for a 5-GHz Device (CLI) 1642
Configuring Event Driven RRM for a CleanAir Event (GUI) 1644
Configuring EDRRM for a CleanAir Event (CLI) 1644
CleanAir Pro Scanning 1645
Feature History for CleanAir Pro Scanning 1645
Information About CleanAir Pro Scanning 1646
Enabling CleanAir Pro Scanning (CLI) 1647
Monitoring CleanAir Pro Statistics (GUI) 1648
Verifying CleanAir Pro Scanning Details 1648
Verifying CleanAir Parameters 1649
Monitoring Interference Devices 1650
Configuration Examples for CleanAir 1650
CleanAir FAQs 1651

CHAPTER 154 **Bluetooth Low Energy** 1653
Information About Bluetooth Low Energy 1653
Enabling Bluetooth Low Energy Beacon (GUI) 1654
Enabling Bluetooth Low Energy Beacon 1654

CHAPTER 155 **Persistent Device Avoidance** 1657
Information about Cisco Persistent Device Avoidance 1657
Configuring Persistent Device Avoidance (GUI) 1658
Configuring Persistent Device Avoidance (CLI) 1658
Verifying Persistent Device Avoidance 1658

CHAPTER 156 **Spectrum Intelligence** 1661

Spectrum Intelligence 1661
Configuring Spectrum Intelligence 1662
Verifying Spectrum Intelligence Information 1662
Debugging Spectrum Intelligence on Supported APs (CLI) 1663

CHAPTER 157 **Spectrum Analysis** 1665
Information About Spectrum Analysis 1665
Live Spectrum Analysis 1666
Performing AP Spectrum Analysis (GUI) 1666
Configuring Spectrum Analysis 1667
Verifying Spectrum Analysis 1667

PART XIII **Mesh Access Points** 1669

CHAPTER 158 **Mesh Access Points** 1671
Introduction to the Mesh Network 1673
Restrictions for Mesh Access Points 1674
MAC Authorization 1676
Preshared Key Provisioning 1676
EAP Authentication 1676
Bridge Group Names 1677
Background Scanning 1678
Information About Background Scanning and MAP Fast Ancestor Find Mode 1678
Mesh Backhaul at 2.4 GHz and 5 GHz 1679
Information About Mesh Backhaul 1679
Information About Mesh Serial Backhaul 1680
Information About Mesh Backhaul RRM 1681
Dynamic Frequency Selection 1682
Country Codes 1682
Intrusion Detection System 1683
Mesh Interoperability Between Controllers 1683
Information About DHCP and NAT Functionality on Root AP (RAP) 1683
Mesh Convergence 1684
Noise-Tolerant Fast 1684

Ethernet Bridging 1684
Multicast Over Mesh Ethernet Bridging Network 1685
Radio Resource Management on Mesh 1686
Air Time Fairness on Mesh 1686
Spectrum Intelligence for Mesh 1687
Indoor Mesh Interoperability with Outdoor Mesh 1687
Workgroup Bridge 1687
Link Test 1688
Mesh Daisy Chaining 1688
Mesh Leaf Node 1689
Flex+Bridge Mode 1689
Backhaul Client Access 1689
Mesh CAC 1689
Prerequisites for Mesh Ethernet Daisy Chaining 1690
Restrictions for Mesh Ethernet Daisy Chaining 1690
Speeding up Mesh Network Recovery Through Fast Detection of Uplink Gateway Reachability Failure 1691
Fast Teardown for a Mesh Deployment 1691
Configuring MAC Authorization (GUI) 1691
Configuring MAC Authorization (CLI) 1692
Configuring MAP Authorization - EAP (GUI) 1693
Configuring MAP Authorization (CLI) 1694
Configuring PSK Provisioning (CLI) 1695
Configuring a Bridge Group Name (GUI) 1696
Configuring a Bridge Group Name (CLI) 1696
Configuring Background Scanning (GUI) 1697
Configuring Background Scanning 1697
Configuring AP Fast Ancestor Find Mode (GUI) 1698
Configuring Background Scanning and MAP Fast Ancestor Find Mode (CLI) 1698
Configuring Backhaul Client Access (GUI) 1699
Configuring Backhaul Client Access (CLI) 1699
Configuring Dot11ax Rates on Mesh Backhaul Per Access Point (GUI) 1700
Configuring Dot11ax Rates on Mesh Backhaul in Mesh Profile (GUI) 1700
Configuring Wireless Backhaul Data Rate (CLI) 1701

Configuring Data Rate Per AP (CLI) 1702
Configuring Data Rate Using Mesh Profile (CLI) 1702
Configuring Mesh Backhaul (CLI) 1703
Configuring Dynamic Frequency Selection (CLI) 1703
Configuring the Intrusion Detection System (CLI) 1704
Configuring Ethernet Bridging (GUI) 1704
Configuring Ethernet Bridging (CLI) 1705
Configuring Multicast Modes over Mesh 1706
Configuring RRM on Mesh Backhaul (CLI) 1707
Configuring RRM Channel Assignment for Root Access Points Globally 1708
1708
Configuring RRM Channel Assignment for an Access Point 1709
Selecting a Preferred Parent (GUI) 1709
Selecting a Preferred Parent (CLI) 1709
Changing the Role of an AP (GUI) 1711
Changing the Role of an AP (CLI) 1711
Configuring the Mesh Leaf Node (CLI) 1711
Configuring the Mesh Leaf Node (GUI) 1712
Configuring Subset Channel Synchronization 1712
Provisioning LSC for Bridge-Mode and Mesh APs (GUI) 1713
Provisioning LSC for Bridge-Mode and Mesh APs 1713
Specifying the Backhaul Slot for the Root AP (GUI) 1714
Specifying the Backhaul Slot for the Root AP (CLI) 1714
Using a Link Test on Mesh Backhaul (GUI) 1715
Using a Link Test on Mesh Backhaul 1715
Configuring Battery State for Mesh AP (GUI) 1716
Configuring Battery State for Mesh AP 1716
Configuring Mesh Convergence (CLI) 1717
Configuring DHCP Server on Root Access Point (RAP) 1717
Configuring Mesh Ethernet Daisy Chaining (CLI) 1718
Enabling Mesh Ethernet Daisy Chaining 1718
Configuring Mesh CAC (CLI) 1719
Configuring ATF on Mesh (GUI) 1719
Configuring ATF on Mesh 1720

Create an ATF Policy for a MAP 1720
Creating an ATF Policy (GUI) 1721
Adding an ATF to a Policy Profile (GUI) 1721
Enabling ATF Mode in an RF Profile (GUI) 1721
Enabling Wireless Mesh Profile 1722
Enabling Serial Backhaul in Radio Profile (GUI) 1722
Enabling Mesh Configurations in Radio Profile (CLI) 1723
Enabling Serial Backhaul (CLI) 1724
Configuration Example for Mesh Serial Backhaul 1725
Associating Wireless Mesh to an AP Profile (CLI) 1725
Configuring Fast Teardown for a Mesh AP Profile (GUI) 1725
Configuring Fast Teardown for a Mesh AP Profile (CLI) 1726
Flex Resilient with Flex and Bridge Mode Access Points 1727
Information About Flex Resilient with Flex and Bridge Mode Access Points 1727
Configuring a Flex Profile (GUI) 1727
Configuring a Flex Profile (CLI) 1728
Configuring a Site Tag (CLI) 1729
Configuring a Mesh Profile (CLI) 1730
Associating Wireless Mesh to an AP Profile (CLI) 1730
Attaching Site Tag to an Access Point (CLI) 1731
Configuring Switch Interface for APs (CLI) 1732
Verifying Flex Resilient with Flex and Bridge Mode Access Points Configuration 1732
Verifying ATF Configuration on Mesh 1733
Verifying Mesh Ethernet Daisy Chaining 1734
Verifying Mesh Convergence 1734
Verifying DHCP Server for Root AP Configuration 1735
Verifying Mesh Backhaul 1735
Verifying Mesh Configuration 1736
Verifying Dot11ax Rates on Mesh Backhaul 1744
Verifying Mesh Serial Backhaul 1744
Verifying the RRM DCA Status 1745
Verifying Fast Teardown with Default Mesh Profile 1745
Verifying Background Scanning and MAP Fast Ancestor Find 1746

CHAPTER 159 **Redundant Root Access Point (RAP) Ethernet Daisy Chaining** 1747

Overview of Redundant RAP Ethernet Daisy Chaining 1747

Prerequisites for Redundant RAP Ethernet Daisy Chaining Support 1748

Configuring Redundant RAP Ethernet Daisy Chaining Support (CLI) 1748

Verifying Daisy Chain Redundancy (CLI) 1748

PART XIV **VideoStream** 1751

CHAPTER 160 **VideoStream** 1753

Information about Media Stream 1753

Prerequisites for Media Stream 1754

How to Configure Media Stream 1754

Configuring Multicast-Direct Globally for Media Stream (CLI) 1754

Configuring Media Stream for 802.11 Bands (CLI) 1755

Configuring a WLAN to Stream Video(GUI) 1757

Configuring a WLAN to Stream Video (CLI) 1757

Deleting a Media Stream (GUI) 1758

Deleting a Media Stream (CLI) 1758

Monitoring Media Streams 1759

Configuring the General Parameters for a Media Stream (GUI) 1760

Adding Media Stream (CLI) 1760

Enabling a Media Stream per WLAN (GUI) 1761

Enabling a Media Stream per WLAN (CLI) 1761

Configuring the General Parameters for a Media Stream (GUI) 1762

Configuring the General Parameters for a Media Stream (CLI) 1762

Configuring Multicast Direct Admission Control (GUI) 1763

Configuring Multicast Direct Admission Control (CLI) 1764

Create and Attach Policy-based QoS Profile 1765

Create a QoS Profile (GUI) 1766

Create a QoS Profile (CLI) 1766

Create a Service Template (GUI) 1767

Create a Service Template (CLI) 1767

Map the Service Template to the Policy Map (GUI) 1768

Map the Service Template to the Policy Map (CLI) 1769
Map the Policy Map (GUI) 1770
Map the Policy Map (CLI) 1770
Viewing Media Stream Information 1771

PART XV Software-Defined Access Wireless 1775

CHAPTER 161 Software-Defined Access Wireless 1777
Information to Software-Defined Access Wireless 1777
Information About SD-Access Wireless Mesh Inter Fabric Edge Switch Roaming Protection 1780
Configuring SD-Access Wireless 1782
Configuring Default Map Server (GUI) 1783
Configuring Default Map Server (CLI) 1783
Configuring SD-Access Wireless Profile (GUI) 1783
Configuring SD-Access Wireless Profile (CLI) 1784
Configuring Map Server in Site Tag (GUI) 1784
Configuring Map Server in Site Tag (CLI) 1785
Configuring Map Server per L2-VNID (GUI) 1785
Configuring Map Server per L2-VNID (CLI) 1786
Verifying SD-Access Wireless 1786

CHAPTER 162 Passive Client 1789
Information About Passive Clients 1789
Enabling Passive Client on WLAN Policy Profile (GUI) 1790
Enabling Passive Client on WLAN Policy Profile (CLI) 1790
Enabling ARP Broadcast on VLAN (GUI) 1791
Enabling ARP Broadcast on VLAN (CLI) 1791
Configuring Passive Client in Fabric Deployment 1792
Enabling Broadcast Underlay on VLAN 1792
Enabling ARP Flooding 1794
Verifying Passive Client Configuration 1795

CHAPTER 163 Fabric in a Box with External Fabric Edge 1797
Introduction to Fabric in a Box with External Fabric Edge 1797

Configuring a Fabric Profile (CLI) 1797
Configuring a Policy Profile (CLI) 1798
Configuring a Site Tag (CLI) 1799
Configuring a WLAN (CLI) 1800
Configuring a Policy Tag (CLI) 1800
Configuring an AP Profile 1801
Configuring Map Server and AP Subnet (CLI) 1801
Configuring Fabric on FiaB Node 1802
Configuring a Fabric Edge Node 1808
Verifying Fabric Configuration 1815

PART XVI VLAN 1821

CHAPTER 164 VLANs 1823
Information About VLANs 1823
Logical Networks 1823
Supported VLANs 1823
VLAN Port Membership Modes 1823
VLAN Configuration Files 1824
Normal-Range VLAN Configuration Guidelines 1825
Extended-Range VLAN Configuration Guidelines 1825
Prerequisites for VLANs 1826
Restrictions for VLANs 1826
How to Configure VLANs 1827
How to Configure Normal-Range VLANs 1827
Creating or Modifying an Ethernet VLAN 1827
Assigning Static-Access Ports to a VLAN (GUI) 1828
Assigning Static-Access Ports to a VLAN 1828
How to Configure Extended-Range VLANs 1829
Creating an Extended-Range VLAN (GUI) 1830
Creating an Extended-Range VLAN 1830
Monitoring VLANs 1831

CHAPTER 165 VLAN Groups 1833

Information About VLAN Groups 1833
Prerequisites for VLAN Groups 1834
Restrictions for VLAN Groups 1834
Creating a VLAN Group (GUI) 1834
Creating a VLAN Group (CLI) 1835
Adding a VLAN Group to Policy Profile (GUI) 1835
Adding a VLAN Group to a Policy Profile 1836
Viewing the VLANs in a VLAN Group 1836
VLAN Group Support for DHCP and Static IP Clients 1837
Supported Features 1837

PART XVII WLAN 1839

CHAPTER 166 WLANs 1841
Information About WLANs 1841
Band Selection 1842
Off-Channel Scanning Deferral 1842
DTIM Period 1842
WLAN Radio Policy 1843
Restrictions for WLAN Radio Policy 1843
Prerequisites for Configuring Cisco Client Extensions 1843
Peer-to-Peer Blocking 1844
Diagnostic Channel 1844
Prerequisites for WLANs 1844
Restrictions for WLANs 1844
How to Configure WLANs 1846
WLAN Wizard 1846
Local Mode 1846
FlexConnect Mode 1850
Guest CWA Mode 1854
Creating WLANs (GUI) 1857
Creating WLANs (CLI) 1857
Deleting WLANs (GUI) 1858
Deleting WLANs 1858

Searching WLANs (CLI) 1859
Enabling WLANs (GUI) 1859
Enabling WLANs (CLI) 1860
Disabling WLANs (GUI) 1860
Disabling WLANs (CLI) 1860
Configuring General WLAN Properties (CLI) 1861
Configuring Advanced WLAN Properties (CLI) 1862
Configuring Advanced WLAN Properties (GUI) 1864
Configuring WLAN Radio Policy (GUI) 1866
Configuring a WLAN Radio Policy (CLI) 1867
Verifying WLAN Properties (CLI) 1868
Verifying WLAN-VLAN Information for an AP 1868
Verifying a WLAN Radio Policy 1869

CHAPTER 167 WLAN Security 1871
Information About WPA1 and WPA2 1871
Information About AAA Override 1872
Configuring AAA Override 1872
Information About VLAN Override 1873
Configuring Override VLAN for Central Switching 1873
Configuring Override VLAN for Local Switching 1874
VLAN Override on Layer 3 Web Authentication 1875
Verifying VLAN Override on Layer 3 Web Authentication 1875
Prerequisites for Layer 2 Security 1875
Restrictions for WPA2 and WP3 1876
Feature History for Fallback for AAA-Overridden VLAN 1876
Information About Fallback for AAA- Overridden VLAN 1877
Central Switching and FlexConnect Mode Scenarios 1877
Configuring Fallback for AAA-Overridden VLAN (CLI) 1878
Verifying Fallback for AAA-Overridden VLAN 1878
How to Configure WLAN Security 1879
Configuring Static WEP Layer 2 Security Parameters (GUI) 1879
Configuring Static WEP Layer 2 Security Parameters (CLI) 1879
Configuring WPA + WPA2 Layer 2 Security Parameters (GUI) 1881

Configuring WPA + WPA2 Layer 2 Security Parameters (CLI) 1881

CHAPTER 168 Remote LANs 1885

Information About Remote LANs 1885
Configuring Remote LANs (RLANs) 1887
Enabling or Disabling all RLANs 1887
Creating RLAN Profile (GUI) 1888
Creating RLAN Profile (CLI) 1888
Configuring RLAN Profile Parameters (GUI) 1889
Configuring RLAN Profile Parameters (CLI) 1889
Creating RLAN Policy Profile (GUI) 1891
Creating RLAN Policy Profile (CLI) 1891
Configuring RLAN Policy Profile Parameters (GUI) 1891
Configuring RLAN Policy Profile Parameters (CLI) 1893
Configuring Policy Tag and Mapping an RLAN Policy Profile to an RLAN Profile (CLI) 1895
Configuring LAN Port (CLI) 1896
Attaching Policy Tag to an Access Point (GUI) 1896
Attaching Policy Tag to an Access Point (CLI) 1896
Verifying RLAN Configuration 1897
Information About RLAN Authentication Fallback 1900
Configuring RLAN Authentication Fallback (CLI) 1900
Modifying 802.1X EAP Timers for RLAN Clients 1901
Verifying RLAN Authentication Fallback 1902

CHAPTER 169 RLAN External Module 1903

Information About External Module 1903
Prerequisites for Configuring External Module 1903
Configuring External Module (GUI) 1903
Configuring External Module (CLI) 1904
Verifying External Module 1904

CHAPTER 170 802.11ax Per WLAN 1905

Information About 802.11ax Mode Per WLAN 1905
Configuring 802.11ax Mode Per WLAN (GUI) 1905

Configuring 802.11ax Mode Per WLAN (CLI) 1906
Verifying 802.11ax Mode Per WLAN 1906

CHAPTER 171 BSS Coloring 1909
Information About BSS Coloring 1909
BSS Coloring 1910
OBSS-PD and Spatial Reuse 1910
Configuring BSS Color on AP (GUI) 1910
Configuring BSS Color in the Privileged EXEC Mode 1911
Configuring BSS Color Globally (GUI) 1911
Configuring BSS Color in the Configuration Mode 1912
Configuring Overlapping BSS Packet Detect (GUI) 1912
Configuring OBSS-PD Spatial Reuse Globally (CLI) 1913
Configuring OBSS PD in an RF Profile (GUI) 1913
Configuring OBSS-PD Spatial Reuse in the RF Profile Mode (CLI) 1914
Verifying BSS Color and OBSS-PD 1914

CHAPTER 172 DHCP for WLANs 1917
Information About Dynamic Host Configuration Protocol 1917
Internal DHCP Servers 1917
External DHCP Servers 1918
DHCP Assignments 1918
DHCP Option 82 1919
Restrictions for Configuring DHCP for WLANs 1920
Guidelines for DHCP Relay Configuration 1920
How to Configure DHCP for WLANs 1921
Configuring DHCP Scopes (GUI) 1921
Configuring DHCP Scopes (CLI) 1922
Configuring the Internal DHCP Server 1923
Configuring the Internal DHCP Server Under Client VLAN SVI (GUI) 1923
Configuring the Internal DHCP Server Under Client VLAN SVI (CLI) 1923
Configuring the Internal DHCP Server Under a Wireless Policy Profile (GUI) 1926
Configuring the Internal DHCP Server Under a Wireless Policy Profile 1926
Configuring the Internal DHCP Server Globally (GUI) 1929

Configuring the Internal DHCP Server Globally (CLI) 1929
Configuring IP Reservations in the Internal DHCP Server (CLI) 1931
Verifying Internal DHCP Configuration 1932
Configuring DHCP-Required for FlexConnect 1933
Information About FlexConnect DHCP-Required 1933
Restrictions and Limitations for FlexConnect DHCP-Required 1934
Configuring FlexConnect DHCP-Required (GUI) 1934
Configuring FlexConnect DHCP-Required (CLI) 1934
Verifying FlexConnect DHCP-Required 1935

CHAPTER 173 **Aironet Extensions IE (CCX IE)** 1937
Information About Aironet Extensions Information Element 1937
Configuring Aironet Extensions IE (GUI) 1937
Configuring Aironet Extensions IE (CLI) 1937
Verifying the Addition of AP Name 1938

CHAPTER 174 **Device Analytics** 1941
Device Analytics 1941
Information About Device Analytics 1941
Restrictions for Device Analytics 1941
Configuring Device Analytics (GUI) 1942
Configuring Device Analytics (CLI) 1942
Verifying Device Analytics 1943
Verifying Device Analytics Configuration 1944
Adaptive 802.11r 1945
Information About Adaptive 802.11r 1945
Configuring Adaptive 802.11r (GUI) 1946
Verifying Adaptive 802.11r 1946

CHAPTER 175 **Device Classifier Dynamic XML Support** 1947
Feature History for Device Classifier Dynamic XML Support 1947
Information About Device Classifier Dynamic XML Support 1948
Enabling Device Classifier (CLI) 1951
Updating Dynamic XML File 1951

Verifying TLV Values 1952
Clearing Old Classification Cache 1952

CHAPTER 176 BSSID Counters 1955
BSSID Counters 1955
Enabling BSSID Statistics and BSSID Neighbor Statistics 1955
Verifying BSSID Statistics on the Controller 1956

CHAPTER 177 Fastlane+ 1959
Information About Fastlane+ 1959
Configuring an Fastlane+ on a WLAN (CLI) 1959
Configuring an Fastlane+ on a WLAN (GUI) 1960
Monitoring Fastlane+ 1960
Verifying Fastlane+ 1961

CHAPTER 178 Workgroup Bridges 1963
Cisco Workgroup Bridges 1963
Configuring Workgroup Bridge on a WLAN 1966
Verifying the Status of a Workgroup Bridge on the Controller 1968
Configuring Access Points as Workgroup Bridge 1968
Turning Cisco Aironet 2700/3700/1572 Series AP into Autonomous Mode 1968
Configuring Cisco Wave 2 APs or 11AX APs in Workgroup Bridge or CAPWAP AP Mode (CLI) 1969
Configure an SSID Profile for Cisco Wave 2 and 11AX APs (CLI) 1969
Configuring the Authentication Server (CLI) 1971
Configuring a Dot1X Credential (CLI) 1971
Configuring an EAP Profile (CLI) 1972
Configuring Manual-Enrollment of a Trustpoint for Workgroup Bridge (CLI) 1973
Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge (CLI) 1974
Configuring Manual Certificate Enrolment Using TFTP Server (CLI) 1976
Importing the PKCS12 Format Certificates from the TFTP Server (CLI) 1977
Configuring Radio Interface for Workgroup Bridges (CLI) 1978
Configuring Workgroup Bridge Timeouts (CLI) 1981
Configuring Bridge Forwarding for Workgroup Bridge (CLI) 1982
Information About Simplifying WGB Configuration 1983

Configuring Multiple WGBs (CLI) 1984
Verifying WGB Configuration 1984

CHAPTER 179 Peer-to-Peer Client Support 1987
Information About Peer-to-Peer Client Support 1987
Configure Peer-to-Peer Client Support 1987

CHAPTER 180 Deny Wireless Client Session Establishment Using Calendar Profiles 1989
Information About Denial of Wireless Client Session Establishment 1989
Configuring Daily Calendar Profile 1990
Configuring Weekly Calendar Profile 1991
Configuring Monthly Calendar Profile 1992
Mapping a Daily Calendar Profile to a Policy Profile 1993
Mapping a Weekly Calendar Profile to a Policy Profile 1994
Mapping a Monthly Calendar Profile to a Policy Profile 1995
Verifying Calendar Profile Configuration 1996
Verifying Policy Profile Configuration 1996

CHAPTER 181 Ethernet over GRE 1999
Introduction to EoGRE 1999
EoGRE Configuration Overview 2000
Create a Tunnel Gateway 2001
Configuring the Tunnel Gateway (GUI) 2002
Configuring a Tunnel Domain 2002
Configuring Tunnel Domain (GUI) 2003
Configuring EoGRE Global Parameters 2004
Configuring EoGRE Global Parameters (GUI) 2004
Configuring a Tunnel Profile 2005
Configuring the Tunnel Profile (GUI) 2006
Associating WLAN to a Wireless Policy Profile 2007
Attaching a Policy Tag and a Site Tag to an AP 2008
Verifying the EoGRE Tunnel Configuration 2008

CHAPTER 182 Wireless Guest Access 2017

Wireless Guest Access 2017
Foreign Map Overview 2020
Wireless Guest Access: Use Cases 2020
Load Balancing Among Multiple Guest Controllers 2021
Guidelines and Limitations for Wireless Guest Access 2021
Troubleshooting IPv6 2021
Configure Mobility Tunnel for Guest Access (GUI) 2022
Configure Mobility Tunnel for Guest Access (CLI) 2022
Configuring Guest Access Policy (GUI) 2022
Configuring Guest Access Policy (CLI) 2023
Viewing Guest Access Debug Information (CLI) 2025
Configure Guest Access Using Different Security Methods 2025
Open Authentication 2025
Configure a WLAN Profile for Guest Access with Open Authentication (GUI) 2025
Configure a WLAN Profile For Guest Access with Open Authentication (CLI) 2026
Configuring a Policy Profile 2027
Local Web Authentication 2027
Configure a Parameter Map (GUI) 2028
Configure a Parameter Map (CLI) 2028
Configure a WLAN Profile for Guest Access with Local Web Authentication (GUI) 2029
Configure a WLAN Profile for Guest Access with Local Web Authentication (CLI) 2029
Configure an AAA Server for Local Web Authentication (GUI) 2030
Configure an AAA Server for Local Web Authentication (CLI) 2030
Global Configuration 2030
Central Web Authentication 2031
Configure a WLAN Profile for Guest Access with Central Web Authentication (GUI) 2031
Configure a WLAN Profile for Guest Access with Central Web Authentication (CLI) 2032
AAA Server Configuration (GUI) 2033
AAA Server Configuration (CLI) 2033
Configuring 802.1x with Local Web Authentication 2034
Configuring Local Web Authentication with PSK Protocol 2035
Central Web Authentication with PSK Protocol 2036
Configure WLAN Profile for Central Web Authentication with PSK Protocol 2037
Central Web Authentication with iPSK Protocol 2037

Configure WLAN Profile for Central Web Authentication with iPSK Protocol 2038
Configure Web Authentication on MAC Address Bypass failure (GUI) 2038
Configure Web Authentication on MAC Address Bypass Failure (CLI) 2038
Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Pre-Shared Key (CLI) 2040
Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with OWE (CLI) 2042
Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Secure Agile Exchange (CLI) 2043
Configuring WLAN for Web Authentication on MAC Authentication Failure with Dot1x (CLI) 2045

CHAPTER 183 **Wired Guest Access** 2047
Information About Wired Guest Access 2047
Restrictions for Wired Guest Access 2050
Configuring Access Switch for Wired Guest Client 2050
Configuring Access Switch for Foreign Controller 2051
Configuring Foreign Controller with Open Authentication (GUI) 2052
Configuring Foreign Controller with Open Authentication 2052
Configuring Foreign Controller with Local Web Authentication (GUI) 2054
Configuring Foreign Controller with Local WEB Authentication 2055
Configuring Anchor Controller with Open Authentication (GUI) 2056
Configuring Anchor Controller with Open Authentication 2057
Configuring Anchor Controller with Local Web Authentication (GUI) 2058
Configuring Anchor Controller with Local Web Authentication 2059
Configuring Session Timeout for a Profile Policy 2060
Global Configuration (GUI) 2061
Verifying Wired Guest Configurations 2061
Wired Guest Access—Use Cases 2065

CHAPTER 184 **Express Wi-Fi by Facebook** 2067
Information About Express Wi-Fi by Facebook 2067
Restrictions for Express Wi-Fi by Facebook 2068
Enabling Express Wi-Fi by Facebook NAC for Policy Profile (GUI) 2068
Enabling Accounting RADIUS Server for Flex Profile (GUI) 2069

Configuring Captive Portal for Express Wi-Fi by Facebook (GUI) 2069
Configuring Captive Portal for Express Wi-Fi by Facebook (CLI) 2069
Configuring Express Wi-Fi by Facebook Policy on Controller (CLI) 2070
Configuring RADIUS Server for Accounting and Authentication in FlexConnect Profile (CLI) 2072
Verifying Express Wi-Fi by Facebook Configurations on Controller 2073
Verifying Express Wi-Fi by Facebook Configurations on the AP 2073

CHAPTER 185 User Defined Network 2077
Information About User Defined Network 2077
Restrictions for User Defined Network 2079
Configuring a User Defined Network 2079
Configuring a User Defined Network (GUI) 2081
Verifying User Defined Network Configuration 2081

CHAPTER 186 Hotspot 2.0 2085
Introduction to Hotspot 2.0 2085
Open Roaming 2087
Configuring Hotspot 2.0 2089
Configuring an Access Network Query Protocol Server 2089
Configuring ANQP Global Server Settings (GUI) 2092
Configuring Open Roaming (CLI) 2092
Configuring Open Roaming (GUI) 2093
Configuring NAI Realms (GUI) 2094
Configuring Organizational Identifier Alias (GUI) 2094
Configuring WAN Metrics (GUI) 2095
Configuring WAN Metrics 2095
Configuring Beacon Parameters (GUI) 2096
Configuring Authentication and Venue (GUI) 2097
Configuring 3GPP/Operator (GUI) 2098
Configuring OSU Provider (GUI) 2099
Configuring an Online Sign-Up Provider 2100
Configuring Hotspot 2.0 WLAN 2101
Configuring an Online Subscription with Encryption WLAN 2101
Attaching an ANQP Server to a Policy Profile 2102

Configuring Interworking for Hotspot 2.0 2103
Configuring the Generic Advertisement Service Rate Limit 2103
Configuring Global Settings 2104
Configuring Advice of Charge 2104
Configuring Terms and Conditions 2105
Defining ACL and URL Filter in AP for FlexConnect 2106
Configuring an OSEN WLAN (Single SSID) 2108
Verifying Hotspot 2.0 Configuration 2109
Verifying Client Details 2110

CHAPTER 187 Client Roaming Across Policy Profile 2111
Information about Client Roaming Policy Profile 2111
Configuring Client Roaming Across Policy Profile 2112
Verifying Client Roaming Across Policy Profiles 2113

CHAPTER 188 Assisted Roaming 2119
802.11k Neighbor List and Assisted Roaming 2119
Restrictions for Assisted Roaming 2120
How to Configure Assisted Roaming 2120
Configuring Assisted Roaming (GUI) 2120
Configuring Assisted Roaming (CLI) 2121
Verifying Assisted Roaming 2122
Configuration Examples for Assisted Roaming 2122

CHAPTER 189 802.11r BSS Fast Transition 2125
Feature History for 802.11r Fast Transition 2125
Information About 802.11r Fast Transition 2126
Information About 802.11r Fast Transition for SAE (FT-SAE) Authenticated Clients 2127
Restrictions for 802.11r Fast Transition 2128
Monitoring 802.11r Fast Transition (CLI) 2129
Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI) 2130
Configuring 802.11r Fast Transition in an Open WLAN (CLI) 2131
Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI) 2133
Configuring 802.11r Fast Transition on a SAE Security-Enabled WLAN (GUI) 2134

Configuring 802.11r Fast Transition on an SAE Security-Enabled WLAN (CLI) 2134
Disabling 802.11r Fast Transition (GUI) 2136
Disabling 802.11r Fast Transition (CLI) 2136
Verifying 802.11r Fast Transition SAE 2136

CHAPTER 190 802.11v 2141
Information About 802.11v 2141
Enabling 802.11v Network Assisted Power Savings 2141
Prerequisites for Configuring 802.11v 2142
Restrictions for 802.11v 2142
Enabling 802.11v BSS Transition Management 2142
Configuring 802.11v BSS Transition Management (GUI) 2143
Configuring 802.11v BSS Transition Management (CLI) 2143

PART XVIII Cisco DNA Service for Bonjour 2145

CHAPTER 191 Cisco DNA Service for Bonjour Solution Overview 2147
About the Cisco DNA Service for Bonjour Solution 2147
Solution Components 2148
Supported Platforms 2149
Supported Network Design 2150
Traditional Wired and Wireless Networks 2150
Wired Networks 2151
Wireless Networks 2153
Cisco SD-Access Wired and Wireless Networks 2154
BGP EVPN Networks 2156

CHAPTER 192 Configuring Local and Wide Area Bonjour Domains 2159
Cisco DNA Service for Bonjour Solution Overview 2159
Restrictions 2159
Cisco Wide Area Bonjour Service Workflow 2160
Cisco Wide Area Bonjour Supported Network Design 2161
Traditional Wired and Wireless Networks 2161
Cisco SD Access Wired and Wireless Networks 2162

Local and Wide Area Bonjour Policies 2162
Default mDNS Service Configurations 2169
HSRP-Aware mDNS Service-Routing 2169
mDNS Service-Gateway SSO Support 2170
Configuring Local and Wide Area Bonjour Domains 2171
How to configure Multicast DNS Mode for LAN and Wired Networks 2171
Enabling mDNS Gateway on the Device 2171
Creating Custom Service Definition (GUI) 2172
Creating Custom Service Definition 2173
Creating Service List (GUI) 2173
Creating Service List 2174
Creating Service Policy (GUI) 2175
Creating Service Policy 2175
Associating Service Policy to an Interface 2176
How to Configure Local Area Bonjour in Multicast DNS Mode for Wireless Networks 2178
Enabling mDNS Gateway on the Device 2179
Creating Custom Service Definition 2181
Creating Service List 2182
Creating Service Policy 2183
Associating Service Policy with Wireless Profile Policy 2184
Configuring Wide Area Bonjour Domain 2185
Enabling mDNS Gateway on the Device 2185
Creating Custom Service Definition 2186
Creating Service List 2187
Creating Service Policy 2188
Associating Service Policy with the Controller in Wide Area Bonjour Domain 2189
Configuring Hot Standby Router Protocol-aware (HSRP-aware) mDNS Service-Routing on SDG 2191
Configuring Hot Standby Router Protocol-aware (HSRP-aware) mDNS Service-Routing on Service-Peer (CLI) 2191
Verifying Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks 2192
Verifying SDG-Agent Status 2192
Verifying Wide Area Bonjour Controller Status 2193
Verifying mDNS Cache Configurations 2194
Verifying Additional mDNS Cache Configurations 2196

Verifying Local Area Bonjour Configuration for LAN and Wireless Networks 2196
Additional References for DNA Service for Bonjour 2197
Feature History for Cisco DNA Service for Bonjour 2197

CHAPTER 193 **Configuring Local Area Bonjour for Wireless Local Mode** 2201
Overview of Local Area Bonjour for Wireless Local Mode 2201
Prerequisites for Local Area Bonjour for Wireless Local Mode 2201
Restrictions for Local Area Bonjour for Wireless Local Mode 2202
Understanding Local Area Bonjour for Wireless Local Mode 2202
Configuring Wireless AP Multicast 2203
Configuring Wireless AP Multicast (GUI) 2204
Configuring Wireless AP Multicast (CLI) 2204
Configuring Multicast in IP Network (CLI) 2205
Configuring Local Area Bonjour for Wireless Local Mode 2206
Configuring mDNS Service Policy (GUI) 2206
Configuring mDNS Service Policy (CLI) 2207
Configuring Custom Service Definition (GUI) 2209
Configuring Custom Service Definition (CLI) 2210
Configuring mDNS Gateway on WLAN (GUI) 2210
Configuring mDNS Gateway on WLAN (CLI) 2211
Configuring Service-Routing on Service-Peer 2211
Configuring Location-Based mDNS on Service-Peer (GUI) 2213
Configuring Location-Based mDNS on Service-Peer (CLI) 2215
Verifying mDNS Gateway Configuration 2217
Reference 2219

CHAPTER 194 **Configuring Local Area Bonjour for Wireless FlexConnect Mode** 2221
Overview of Local Area Bonjour for Wireless FlexConnect Mode 2221
Restrictions for Local Area Bonjour for Wireless FlexConnect Mode 2221
Prerequisites for Local Area Bonjour for Wireless FlexConnect Mode 2222
Understanding mDNS Gateway Alternatives for Wireless FlexConnect Mode 2222
Understanding Local Area Bonjour for Wireless FlexConnect Mode 2224
Configuring Local Area Bonjour for Wireless FlexConnect Mode 2226
Configuring mDNS Gateway Mode (CLI) 2226

Configuring mDNS Service Policy (CLI) 2227
Configuring mDNS Location-Filter (CLI) 2231
Configuring Custom Service Definition (CLI) 2234
Configuring Service-Routing on Service-Peer (CLI) 2235
Configuring Location-Based mDNS 2237
Configuring Service-Routing on SDG Agent (CLI) 2237
Verifying Local Area Bonjour in Service-Peer Mode 2239
Verifying Local Area Bonjour in SDG Agent Mode 2241
Reference 2243

CHAPTER 195 **Configuration Example for Local Mode - Wireless and Wired** 2245
Overview 2245
Configuring Wireless AP Multicast Mode 2246
Configuration Example for Default Service List and Policy in Wide Area Bonjour Between Multilayer Wired and Wireless Endpoints 2247
Example: Wired and Wireless Access Layer Service Peer Configuration 2247
Example: Wired and Wireless Distribution Layer SDG Agent Configuration 2248
Configuration Example for Customized Service List and Policy in Wide Area Bonjour Between Multilayer Wired and Wireless Endpoints 2249
Example: Wired and Wireless Access Layer Service Peer Configuration 2249
Example: Wired and Wireless Distribution Layer SDG Agent Configuration 2251
Cisco Catalyst Center Traditional Multilayer Wired and Wireless Configuration 2252
Configuring Service Filters for Traditional Multilayer Wired and Wireless - Local Mode (GUI) 2252
Configuring Source SDG Agents in Traditional Multilayer Wired and Wireless - Local Mode (GUI) 2253
Configuring Query SDG Agents in Traditional Multilayer Wired and Wireless - Local Mode (GUI) 2253
Verifying Wide Area Bonjour Between Multilayer Wired and Wireless Local Mode 2254
Verifying Wired Service-Peer Configuration 2254
Verifying Wired SDG Agent Configuration and Service-Routing Status 2256
Verifying Wireless Service-Peer Configuration and Service Status 2258
Verifying Wireless SDG Agent Configuration and Service-Routing Status 2259
Verifying Cisco Catalyst Center Configuration and Service-Routing Status 2260
Reference 2261

CHAPTER 196 **Configuration Example for FlexConnect Mode - Wireless and Wired** 2263

Overview 2263

Configuration Example for Default Service List and Policy in FlexConnect Mode - Wireless and Wired 2264

Example: Wired and Wireless Access Layer Service Peer Configuration 2264

Example: Wired and Wireless Distribution Layer SDG Agent Configuration 2266

Configuration Example for Customized Service List and Policy in FlexConnect Mode - Wireless and Wired 2267

Example: Wired and Wireless Access Layer Service Peer Configuration 2267

Example: Wired and Wireless Distribution Layer SDG Agent Configuration 2268

Cisco Catalyst Center Traditional Multilayer Wired and Wireless Configuration 2269

Configuring Service Filters for Traditional Multilayer Wired and Wireless FlexConnect Local-Switching Mode (GUI) 2269

Configuring Source SDG Agents in Traditional Multilayer Wired and Wireless FlexConnect Local-Switching Mode (GUI) 2270

Configuring Query SDG Agents in Traditional Multilayer Wired and Wireless FlexConnect Local-Switching Mode (GUI) 2271

Verifying Configuration Example for FlexConnect Mode - Wireless and Wired 2271

Verifying Wired Service-Peer Configuration 2271

Verifying Wired SDG Agent Configuration and Service-Routing Status 2273

Verifying Cisco Catalyst Center Configuration and Service Routing Status 2275

Reference 2275

PART XIX **Multicast Domain Name System** 2277

CHAPTER 197 **Multicast Domain Name System** 2279

Introduction to mDNS Gateway 2280

Guidelines and Restrictions for Configuring mDNS AP 2280

Enabling mDNS Gateway (GUI) 2282

Enabling or Disabling mDNS Gateway (GUI) 2282

Enabling or Disabling mDNS Gateway (CLI) 2283

Creating Default Service Policy 2284

Creating Custom Service Definition (GUI) 2285

Creating Custom Service Definition 2285

Creating Service List (GUI) 2286
Creating Service List 2287
Creating Service Policy (GUI) 2288
Creating Service Policy 2289
Configuring a Local or Native Profile for an mDNS Policy 2291
Configuring an mDNS Flex Profile (GUI) 2291
Configuring an mDNS Flex Profile (CLI) 2292
Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (GUI) 2292
Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (CLI) 2293
Enabling the mDNS Gateway on the VLAN Interface 2293
Location-Based Service Filtering 2294
Prerequisite for Location-Based Service Filtering 2294
Configuring mDNS Location-Based Filtering Using SSID 2294
Configuring mDNS Location-Based Filtering Using AP Name 2295
Configuring mDNS Location-Based Filtering Using AP Location 2296
Configuring mDNS Location-Based Filtering Using Regular Expression 2296
Configuring mDNS Location-Based Filtering Using Location Group 2297
Feature History for mDNS Location-Based Filtering Using Location Group (Microlocation) 2297
Information About mDNS Location-Based Filtering Using Location Group (Microlocation) 2297
Use Cases for mDNS Location-Based Filtering Using Location Group (Microlocation) 2298
Prerequisites for mDNS Location-Based Filtering Using Location Group (Microlocation) 2298
Enabling Location Group (CLI) 2298
Adding APs to a Location Group (CLI) 2299
Verifying AP Location 2301
Nearest mDNS-Based Wired Service Filtering 2301
Feature History for Nearest mDNS-Based Wired Service Filtering 2301
Information About Nearest mDNS-Based Wired Service Filtering 2302
Information About Custom Wired Service Policy Support for FlexConnect Mode 2304
Information About VLAN and MAC Based Wired Service Filtering 2304
Prerequisite for Nearest mDNS-Based Wired Service Filtering 2305
Use Cases 2305
Configuring Wired Service Policy Support in Flex Profile 2305
Creating Service List (CLI) 2305
Creating Service Policy (CLI) 2307

Configuring an mDNS Flex Profile (GUI) 2307
Configuring an mDNS Flex Profile (CLI) 2308
Configuring VLAN and MAC Based Wired Service Filtering (CLI) 2309
Verifying mDNS-Based Wired Service Filtering 2311
Configuring mDNS AP 2312
Enabling mDNS Gateway on the RLAN Interface 2313
Enabling mDNS Gateway on Guest LAN Interface 2316
Associating mDNS Service Policy with Wireless Profile Policy (GUI) 2317
Associating mDNS Service Policy with Wireless Profile Policy 2317
Enabling or Disabling mDNS Gateway for WLAN (GUI) 2320
Enabling or Disabling mDNS Gateway for WLAN 2321
mDNS Gateway with Guest Anchor Support and mDNS Bridging 2322
Configuring mDNS Gateway on Guest Anchor 2322
Configuring mDNS Gateway on Guest Foreign (Guest LAN) 2323
Configuring mDNS Gateway on Guest Anchor 2323
Configuring mDNS Gateway on Guest Foreign (Guest WLAN) 2324
Verifying mDNS Gateway Configurations 2324

Preface

This preface describes the conventions of this document and information on how to obtain other documentation. It also provides information on what's new in Cisco product documentation.

- Document Conventions , on page xcvii
- Related Documentation, on page xcix
- Communications, Services, and Additional Information, on page xcix

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^**D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier` font	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number provided at the end of each warning statement to locate its translation in the translated safety warnings for this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

Note Before installing or upgrading the device, refer to the release notes at https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html.

- Cisco Catalyst 9800-40 Wireless Controller documentation, located at:

  http://www.cisco.com/go/c9800

- Cisco Catalyst 9800-80 Wireless Controller documentation, located at:

  http://www.cisco.com/go/c9800

- Cisco Catalyst 9800-L Wireless Controller documentation, located at:

  http://www.cisco.com/go/c9800

Communications, Services, and Additional Information

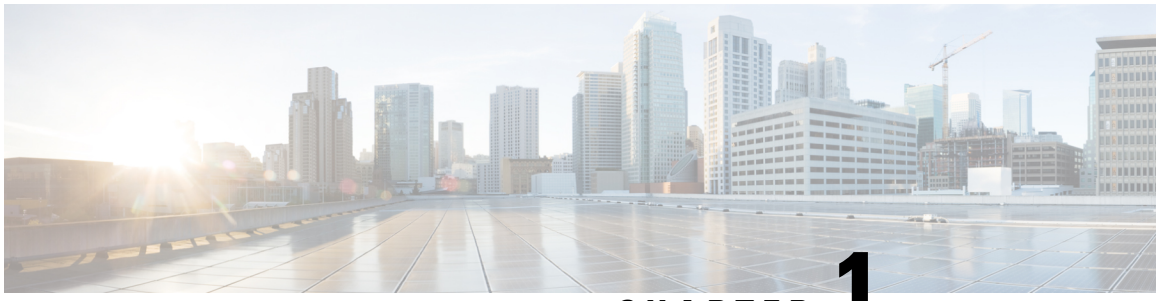
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



CHAPTER 1

Overview of the Controller

- Overview of Cisco 9800 Series Wireless Controllers , on page 1
- Elements of the New Configuration Model, on page 1
- Configuration Workflow, on page 2
- Initial Setup, on page 3
- Interactive Help, on page 4

Overview of Cisco 9800 Series Wireless Controllers

Cisco Catalyst 9800 Series Wireless Controllers are the next generation of wireless controllers built for the Intent-based networking. The Cisco Catalyst 9800 Series Controllers are IOS XE based and integrates the RF Excellence from Aironet with Intent-based Networking capabilities of IOS XE to create the best-in-class wireless experience for your evolving and growing organization.

The controllers are deployable in physical and virtual (private and public cloud) form factors and can be managed using Cisco Catalyst Center, Netconf/YANG, Cisco Prime Infrastructure, web-based GUI, or CLI.

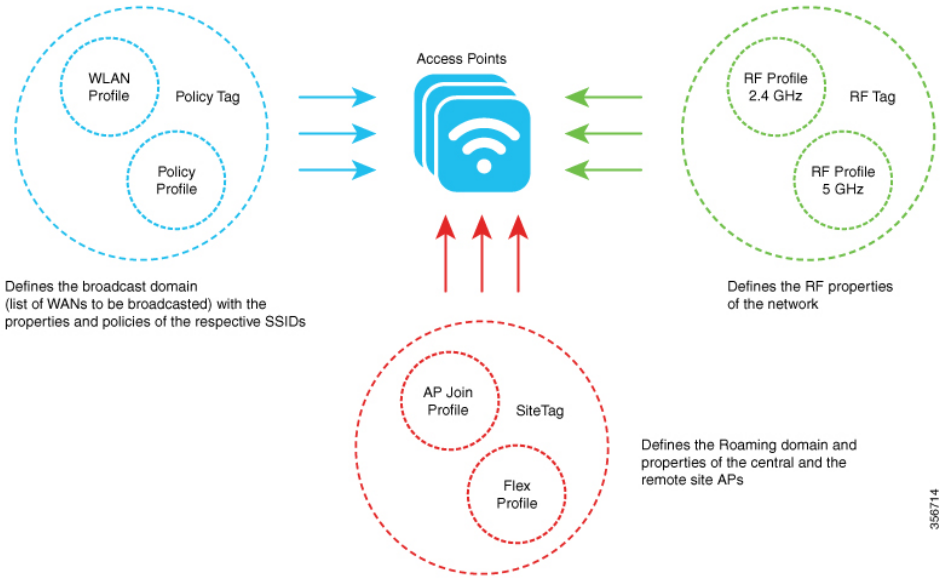
The Cisco Catalyst 9800 Series Wireless Controllers are available in multiple form factors to cater to your deployment options:

- Cisco Catalyst 9800 Series Wireless Controller Appliance
- Cisco Catalyst 9800 Series Wireless Controller for Cloud
- Cisco Catalyst 9800 Embedded Wireless for Switch

The configuration data model is based on design principles of reusability, simplified provisioning, enhanced flexibility and modularization to help manage networks as they scale up and simplify the management of dynamically changing business and IT requirements.

Elements of the New Configuration Model

The following diagram depicts the elements of the new configuration model.



Tags

The property of a tag is defined by the property of the policies associated to it, which in turn is inherited by an associated client or an AP. There are various type of tags, each of which is associated to different profiles. Every tag has a default that is created when the system boots up.

Profiles

Profiles represent a set of attributes that are applied to the clients associated to the APs or the APs themselves. Profiles are reusable entities that can be used across tags.

Configuration Workflow

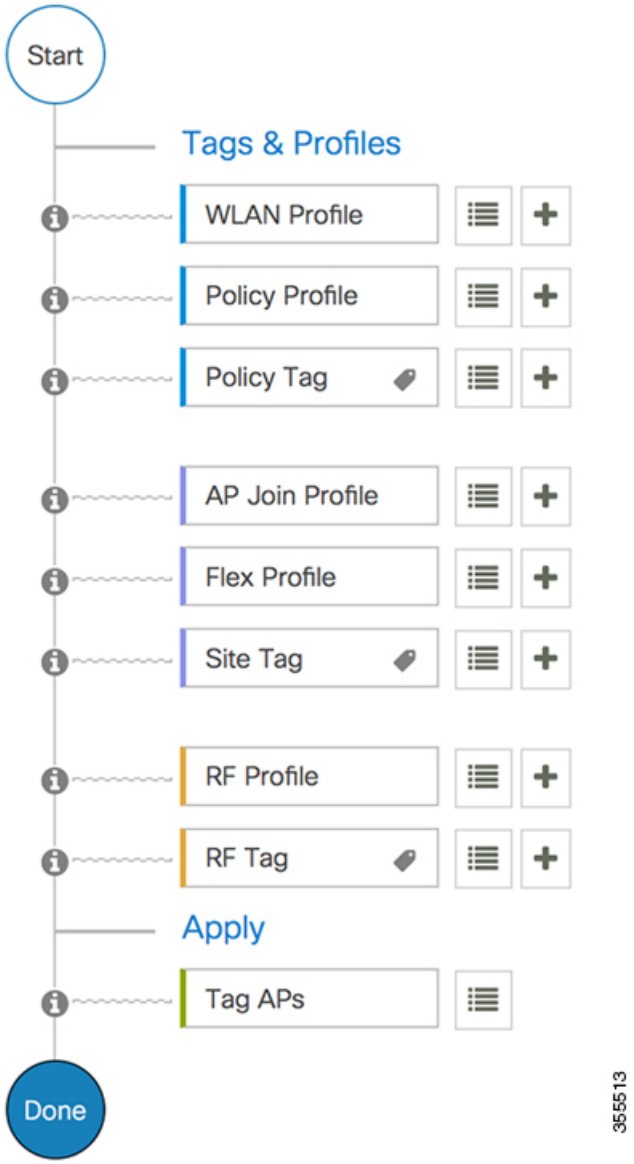
The following set of steps defines the logical order of configuration. Apart from the WLAN profile, all the profiles and tags have a default object associated with it.

1. Create the following profiles:
    - WLAN
    - Policy
    - AP Join
    - Flex
    - RF
2. Create the following tags:
    - Policy
    - Site

- RF

3. Associate tags to an AP.

Figure 1: Configuration Workflow



Initial Setup

Setting up the Controller

The initial configuration wizard in Cisco Catalyst 9800 Series Wireless Controller is a simplified, out-of-the-box installation and configuration interface for controller. This section provides instructions to set up a controller

to operate in a small, medium, or large network wireless environment, where access points can join and together as a simple solution provide various services, such as corporate employee or guest wireless access on the network.

Setting Up the Controller Using GUI

To set up the controller using GUI, see the *Configuring Wireless Controller* section in Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide.

Note

- If you make configuration changes in the Command Line Interface (CLI) and in the GUI simultaneously, you must click the **Refresh** button in the GUI to synch both the changes. You should always click the **Refresh** button in the GUI, to update the changes done through CLI.
- The banner text is fetched from the controller when you land on the login page. You will be able to see this request on the RADIUS server.
- When you log in to the Cisco Catalyst 9800-L Wireless Controller GUI, you will receive a large number CPU alerts due to CPU utilization spike during log in.

Setting Up the Controller Using CLI

To set up the controller using CLI, see the *Performing the Initial Configuration on the Controller* section of your respective controller installation guides.

- Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide
- Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide
- Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide
- Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide
- Cisco Catalyst CW9800M Wireless Controller Hardware Installation Guide
- Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers Hardware Installation Guide

Interactive Help

The Cisco Catalyst 9800 Series Wireless Controller GUI features an interactive help that walks you through the GUI and guides you through complex configurations.

You can start the interactive help in the following ways:

- By hovering your cursor over the blue flap at the right-hand corner of a window in the GUI and clicking **Interactive Help**.
- By clicking **Walk-me Thru** in the left pane of a window in the GUI.
- By clicking **Show me How** displayed in the GUI. Clicking **Show me How** triggers a specific interactive help that is relevant to the context you are in.

For instance, **Show me How** in **Configure** > **AAA** walks you through the various steps for configuring a RADIUS server. Choose **Configuration**> **Wireless Setup** > **Advanced** and click **Show me How** to trigger the interactive help that walks you through the steps relating to various kinds of authentication.

The following features have an associated interactive help:

- Configuring AAA
- Configuring FlexConnect Authentication
- Configuring 802.1x Authentication
- Configuring Local Web Authentication
- Configuring OpenRoaming
- Configuring Mesh APs

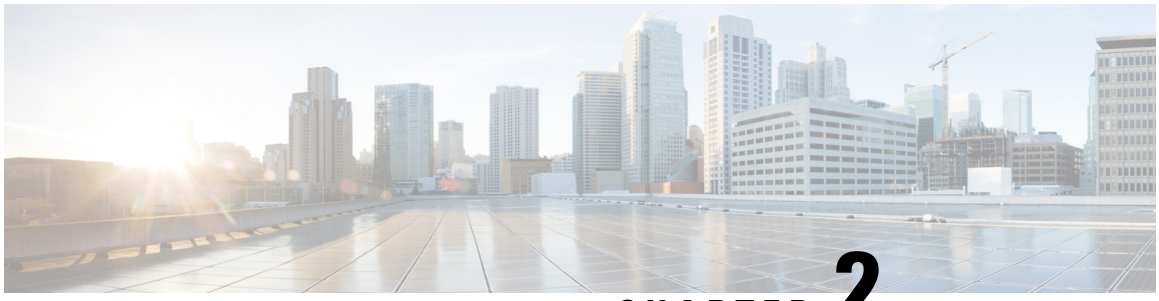
Note If the WalkMe launcher is unavailable on Safari, modify the settings as follows:

1. Choose **Preferences > Privacy**.
2. In the **Website tracking** section, uncheck the **Prevent cross-site tracking** check box to disable this action.
3. In the **Cookies and website data** section, uncheck the **Block all cookies** check box to disable this action.

PART I

System Configuration

- New Configuration Model, on page 9
- Wireless Management Interface, on page 47
- BIOS Protection, on page 57
- Smart Licensing Using Policy, on page 59
- Management over Wireless, on page 181
- Boot Integrity Visibility, on page 183
- SUDI99 Certificate Support, on page 187
- Link Aggregation Group, on page 191
- Best Practices, on page 201



CHAPTER 2

New Configuration Model

- Information About New Configuration Model, on page 9
- Configuring a Wireless Profile Policy (GUI), on page 12
- Configuring a Wireless Profile Policy (CLI), on page 12
- Configuring a Flex Profile (GUI), on page 14
- Configuring a Flex Profile, on page 14
- Configuring an AP Profile (GUI), on page 15
- Configuring an AP Profile (CLI), on page 20
- Configuring User for AP Management (CLI), on page 21
- Setting a Private Configuration Key for Password Encryption, on page 21
- Configuring an RF Profile (GUI), on page 22
- Configuring an RF Profile (CLI), on page 22
- Configuring a Site Tag (GUI), on page 24
- Configuring a Site Tag (CLI), on page 24
- Enhanced Site Tag-Based Load Balancing, on page 25
- Configuring Policy Tag (GUI), on page 28
- Configuring a Policy Tag (CLI), on page 28
- Configuring Wireless RF Tag (GUI), on page 29
- Configuring Wireless RF Tag (CLI), on page 30
- Attaching a Policy Tag and Site Tag to an AP (GUI), on page 31
- Attaching Policy Tag and Site Tag to an AP (CLI), on page 31
- Configuring a Radio Profile, on page 32
- AP Filter, on page 36
- Configuring Access Point for Location Configuration, on page 41

Information About New Configuration Model

The configuration of Cisco Catalyst 9800 Series Wireless Controllers is simplified using different tags, namely rf-tag, policy-tag, and site-tag. The access points would derive their configuration from the profiles that are contained within the tags.

Profiles are a collection of feature-specific attributes and parameters applied to tags. The rf-tag contains the radio profiles, the site-tag contains flex-profile and ap-join-profile, and the policy-tag contains the WLAN profile and policy profile.

The FlexConnect configuration helps the central controller to manage sites that are geo-distributed, for example, retail, campus, and so on.

Policy Tag

The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client (Quality of Service [QoS] is an exception which constitutes AP policies as well).

The policy tag contains the map of WLAN policy profile. There are 16 such entries per policy tag. Changes to the map entries are effected based on the status of the WLAN profile and policy profile. For example, if a map (WLAN1 and Policy1) is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to the APs using the policy tag. However, if one of them is in disabled state, the definition is not pushed to the AP. Similarly, if a WLAN profile is already being broadcast by an AP, it can be deleted using the no form of the command in the policy tag.

Site Tag

The site tag defines the properties of a site and contains the flex profile and the AP join profile. The attributes that are specific to the corresponding flex or remote site are part of the flex profile. Apart from the flex profile, the site tag also comprises attributes that are specific to the physical site (and hence cannot be a part of the profile that is a reusable entity). For example, the list of primary APs for efficient upgrade is a part of a site tag rather than that of a flex profile.

If a flex profile name or an AP profile name is changed in the site tag, the AP is forced to rejoin the controller by disconnecting the Datagram Transport Layer Security (DTLS) session. When a site tag is created, the AP and flex profiles are set to default values (default-ap-profile and default-flex-profile).

RF Tag

The RF tag contains the 2.4 GHz, 5 GHz, and 6 GHz RF profiles. The default RF tag contains the global configuration for 2.4 and 5 GHz bands and default RF profile for 6 GHz band. All these profiles contain the same default values for global or RF profile parameters for the respective radios.

Profiles

Profiles are a collection of feature-specific attributes and parameters applied to tags. Profiles are reusable entities that can be used across tags. Profiles (used by tags) define the properties of the APs or its associated clients.

WLAN Profile

WLAN profiles are configured with same or different service set identifiers (SSIDs). An SSID identifies the specific wireless network for the controller to access. Creating WLANs with the same SSID allows to assign different Layer 2 security policies within the same wireless LAN.

To distinguish WLANs having the same SSID, create a unique profile name for each WLAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can select a WLAN based on the information advertised in the beacon and probe responses. The switching and network policies are not part of the WLAN definition.

Policy Profile

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for a client that is applied on an AP or controller is moved to the policy profile, for example, VLAN, ACL, QoS, session timeout, idle timeout, AVC profile, bonjour profile, local profiling, device classification, BSSID QoS, and so on. However, all the wireless-related security attributes and features on the WLAN are grouped under the WLAN profile.

Flex Profile

Flex profile contains policy attributes and remote site-specific parameters. For example, the EAP profiles that can be used when the AP acts as an authentication server for local RADIUS server information, VLAN-ACL mapping, VLAN name-to-ID mapping, and so on.

AP Join Profile

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4 and IPv6, UDP Lite, High Availability, Retransmit config parameters, Global AP failover, Hyperlocation config parameters, Telnet and SSH, 11u parameters, and so on.

Note Telnet is not supported for the following Cisco AP models: 1542D, 1542I, 1562D, 1562E, 1562I, 1562PS, 1800S, 1800T, 1810T, 1810W,1815M, 1815STAR, 1815TSN, 1815T, 1815W, 1832I, 1840I, 1852E, 1852I, 2802E, 2802I, 2802H, 3700C, 3800, 3802E, 3802I, 3802P, 4800, IW6300, ESW6300, 9105AXI, 9105AXW, 9115AXI, 9115AXE, 9117I, APVIRTUAL, 9120AXI, 9120AXE, 9124AXI, 9124AXD, 9130AXI, 9130AXE, 9136AXI, 9162I, 9164I, and 9166I.

RF Profile

RF profile contains the common radio configuration for the APs. RF profiles are applied to all the APs that belong to an AP group, where all the APs in that group have the same profile settings.

Some of the 6-GHz band specific 802.11ax features like Unsolicited Broadcast Probe Response, FILS Discovery, Multi-BSSID reduce the overhead of management traffic in 6-GHz band channels. Preferred Scanning Channels is another feature in 6-GHz band which helps RRM to choose PSC channels to 6-GHz radios.

Association of APs

APs can be associated using different ways. The default option is by using Ethernet MAC address, where the MAC is associated with policy-tag, site tag, and RF tag.

In filter-based association, APs are mapped using regular expressions. A regular expression (regex) is a pattern to match against an input string. Any number of APs matching that regex will have policy-tag, site tag, and RF tag mapped to them, which is created as part of the AP filter.

In AP-based association, tag names are configured at the PnP server and the AP stores them and sends the tag name as part of discovery process.

In location-based association, tags are mapped as per location and are pushed to any AP Ethernet MAC address mapped to that location.

Modifying AP Tags

Modifying an AP tag results in DTLS connection reset, forcing the AP to rejoin the controller. If only one tag is specified in the configuration, default tags are used for other types, for example, if only policy tag is specified, the default-site-tag and default-rf-tag will be used for site tag and RF tag.

Configuring a Wireless Profile Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click **Add**.

Step 3 In the **Add Policy Profile** window, in **General** tab, enter a name and description for the policy profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces. Do not use spaces as it causes system instability.

Step 4 To enable the policy profile, set **Status** as **Enabled**.

Step 5 Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.

Step 6 In the **CTS Policy** section, choose the appropriate status for the following:

- Inline Tagging—a transport mechanism using which a controller or access point understands the source SGT.
- SGACL Enforcement

Step 7 Specify a default **SGT**. The valid range is from 2 to 65519.

Step 8 In the WLAN Switching Policy section, choose the following, as required:

- Central Switching: Tunnels both the wireless user traffic and all control traffic via CAPWAP to the centralized controller where the user traffic is mapped to a dynamic interface/VLAN on the controller. This is the normal CAPWAP mode of operation.
- Central Authentication: Tunnels client data to the controller, as the controller handles client authentication.
- Central DHCP: The DHCP packets received from AP are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
- Central Association Enable: When central association is enabled, all switching is done on the controller.
- Flex NAT/PAT: Enables Network Address Translation(NAT) and Port Address Translation (PAT) mode.

Step 9 Click **Save & Apply to Device**.

Configuring a Wireless Profile Policy (CLI)

Follow the procedure given below to configure a wireless profile policy:

Note When a client moves from an old controller to a new controller (managed by Cisco Prime Infrastructure), the old IP address of the client is retained, if the IP address is learned by ARP or data gleaning. To avoid this scenario, ensure that you enable **ipv4 dhcp required** command in the policy profile. Otherwise, the IP address gets refreshed only after a period of 24 hours.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**idle-timeout** *timeout* **Example:** `Device(config-wireless-policy)# idle-timeout 1000`	(Optional) Configures the duration of idle timeout, in seconds.
Step 4	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 24`	Configures VLAN name or VLAN ID.
Step 5	**accounting-list** *list-name* **Example:** `Device(config-wireless-policy)# accounting-list user1-list`	Sets the accounting list for IEEE 802.1x.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 7	**show wireless profile policy summary** **Example:** `Device# show wireless profile policy summary`	Displays the configured policy profiles. **Note** (Optional) To view detailed information about a policy profile, use the **show wireless profile policy detailed** *policy-profile-name* command.

Configuring a Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Flex**.

Step 2 Click **Add**.

Step 3 Enter the **Name** of the Flex Profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 In the **Description** field, enter a description for the Flex Profile.

Step 5 Click **Apply to Device**.

Configuring a Flex Profile

Follow the procedure given below to set a flex profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a Flex profile and enters Flex profile configuration mode.
Step 3	**description** **Example:** `Device(config-wireless-flex-profile)# description xyz-default-flex-profile`	(Optional) Enables default parameters for the flex profile.
Step 4	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	(Optional) Enables ARP caching.
Step 5	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show wireless profile flex summary** **Example:** `Device# show wireless profile flex summary`	(Optional) Displays the flex-profile parameters. **Note** To view detailed parameters about the flex profile, use the **show wireless profile flex detailed** *flex-profile-name* command.

Configuring an AP Profile (GUI)

Before you begin

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4/IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet/SSH, 11u parameters, and so on.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** page, click **Add**.

The **Add AP Join Profile** page is displayed.

Note DHCP fallback is enabled by default. So, if an AP is assigned a static IP address and unable to reach the controller, the AP falls back to the DHCP. To stop an AP from moving the static IP to DHCP, you must disable the DHCP fallback configuration in an AP join profile.

Step 3 In the **General** tab, enter a name and description for the AP join profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Check the **LED State** check box to set the LED state of all APs connected to the device to blink so that the APs are easily located. The LED state is enabled by default.

Step 5 In the **Client** tab and **Statistics Timer** section, enter the time in seconds that the AP sends its 802.11 statistics to the controller.

Step 6 In the **TCP MSS Configuration** section, check the **Adjust MSS Enable** check box to enter value for Adjust MSS. You can enter or update the maximum segment size (MSS) for transient packets that traverse a router. TCP MSS adjustment enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments with the SYN bit set.

In a CAPWAP environment, a lightweight access point discovers a device by using CAPWAP discovery mechanisms, and then sends a CAPWAP join request to the device. The device sends a CAPWAP join response to the access point that allows the access point to join the device.

When the access point joins the device, the device manages its configuration, firmware, control transactions, and data transactions.

Step 7 In the **CAPWAP** tab, you can configure the following:

- High Availability

  You can configure primary and secondary backup controllers for all access points (which are used if primary, secondary, or tertiary controllers are not responsive) in this order: primary, secondary, tertiary, primary backup, and secondary backup. In addition, you can configure various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.

a) In the **High Availability** tab, enter the time (in seconds) in the **Fast Heartbeat Timeout** field to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.

Note Configure **Fast Heartbeat Timeout** to assist AP in sending primary discovery request periodically to the configured backup controllers along with the primary, secondary, and tertiary-base controllers.

b) In the **Heartbeat Timeout** field, enter the time (in seconds) to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.
c) In the **Discovery Timeout** field, enter a value between 1 and 10 seconds (inclusive) to configure the AP discovery request timer.
d) In the **Primary Discovery Timeout** field, enter a value between 30 and 3000 seconds (inclusive) to configure the access point primary discovery request timer.
e) In the **Primed Join Timeout** field, enter a value between 120 and 43200 seconds (inclusive) to configure the access point primed join timeout.
f) In the **Retransmit Timers Count** field, enter the number of times that you want the AP to retransmit the request to the device and vice-versa. Valid range is between 3 and 8.
g) In the **Retransmit Timers Interval** field, enter the time duration between retransmission of requests. Valid range is between 2 and 5.
h) Check the **Enable Fallback** check box to enable fallback.
i) Enter the **Primary Controller** name and IP address.
j) Enter the **Secondary Controller** name and IP address.
k) Click **Save & Apply to Device**.

Note The primary and secondary settings in the AP join profile are not used for AP fallback. This means that the AP will not actively probe for those controllers (which are a part of the AP join profile), when it has joined one of them.

This setting is used only when the AP loses its connection with the controller, and then prioritizes which other controller it should join. These controllers have a priority of 4 and 5, following APs in the **High Availability** tab of the AP page.

The APs that are added as the primary, secondary, and tertiary APs in the **High Availability** tab of the AP configuration page, are actively probed and are used for the AP fallback option.

- Advanced

a) In the **Advanced** tab, check the **Enable VLAN Tagging** check box to enable VLAN tagging.
b) Check the **Enable Data Encryption** check box to enable Datagram Transport Layer Security (DTLS) data encryption.

c) Check the **Enable Jumbo MTU** to enable big maximum transmission unit (MTU). MTU is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before transmission. Jumbo frames are frames that are bigger than the standard Ethernet frame size, which is 1518 bytes (including Layer 2 (L2) header and FCS). The definition of frame size is vendor-dependent, as these are not part of the IEEE standard.

d) Use the **Link Latency** drop-down list to select the link latency. Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the AP to the controller and back.

e) From the **Preferred Mode** drop-down list, choose the mode.

f) Click **Save & Apply to Device**.

Step 8 In the **AP** tab, you can configure the following:

- General

a) In the **General** tab, check the **Switch Flag** check box to enable switches.

b) Check the **Power Injector State** check box if power injector is being used. Power Injector increases wireless LAN deployment flexibility of APs by providing an alternative powering option to local power, inline power-capable multiport switches, and multiport power patch panels.

Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed.

c) From the **Power Injector Type** drop-down list, choose power injector type from the following options:

- Installed—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

  If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address text box. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address text box blank.

  Note Each time an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- Override—This option allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

d) In the **Injector Switch MAC** field, enter the MAC address of the switch either in xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx, or xxxx.xxxx.xxxx format.

e) From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP*.

f) From the **AP Authorization Type** drop-down list, choose the type as either *CAPWAP DTLS* + or *CAPWAP DTLS*.

g) In the **Client Statistics Reporting Interval** section, enter the interval for 5 GHz and 2.4 GHz radios in seconds.

h) Check the **Enable** check box to enable extended module.

i) From the **Profile Name** drop-down list, choose a profile name for mesh.
j) Click **Save & Apply to Device**.

- Hyperlocation: Cisco Hyperlocation is a location solution that allows to track the location of wireless clients with the accuracy of one meter. Selecting this option disables all other fields in the screen, except NTP Server.

a) In the **Hyperlocation** tab, check the **Enable Hyperlocation** check box.
b) Enter the **Detection Threshold** value to filter out packets with low RSSI. The valid range is –100 dBm to –50 dBm.
c) Enter the **Trigger Threshold** value to set the number of scan cycles before sending a BAR to clients. The valid range is 0 to 99.
d) Enter the **Reset Threshold** value to reset value in scan cycles after trigger. The valid range is 0 to 99.
e) Enter the **NTP Server** IP address.
f) Click **Save & Apply to Device**.

- BLE: If your APs are Bluetooth Low Energy (BLE) enabled, they can transmit beacon messages that are packets of data or attributes transmitted over a low energy link. These BLE beacons are frequently used for health monitoring, proximity detection, asset tracking, and in-store navigation. For each AP, you can customize BLE Beacon settings configured globally for all APs.

a) In the **BLE** tab, enter a value in the **Beacon Interval** field to indicate how often you want your APs to send out beacon advertisements to nearby devices. The range is from 1 to 10, with a default of 1.
b) In the **Advertised Attenuation Level** field, enter the attenuation level. The range is from 40 to 100, with a default of 59.
c) Click **Save & Apply to Device**.

- Packet Capture: Packet Capture feature allows to capture the packets on the AP for the wireless client troubleshooting. The packet capture operation is performed on the AP by the radio drivers on the current channel on which it is operational, based on the specified packet capture filter.

a) In the **Packet Capture** tab, choose an **AP Packet Capture Profile** from the drop-down list.
b) You can also create a new profile by clicking the + sign.
c) Enter a name and description for the AP packet capture profile.
d) Enter the **Buffer Size**.
e) Enter the **Duration**.
f) Enter the **Truncate Length** information.
g) In the **Server IP** field, enter the IP address of the TFTP server.
h) In the **File Path** field, enter the directory path.
i) Enter the username and password details.
j) From the **Password Type** drop-down list, choose the type.
k) In the **Packet Classifiers** section, use the option to select or enter the packets to be captured.
l) Click **Save**.
m) Click **Save & Apply to Device**.

Step 9 In the **Management** tab, you can configure the following:

- Device

a) In the **Device** tab, enter the **IPv4/IPv6 Address** of the TFTP server, **TFTP Downgrade** section.
b) In the **Image File Name** field, enter the name of the software image file.

c) From the **Facility Value** drop-down list, choose the appropriate facility.
d) Enter the IPv4 or IPv6 address of the host.
e) Choose the appropriate **Log Trap Value**.
f) Enable Telnet and/or SSH configuration, if required.
g) Enable core dump, if required.
h) Click **Save & Apply to Device**.

- User

a) In the **User** tab, enter username and password details.
b) Choose the appropriate password type.
c) In the **Secret** field, enter a custom secret code.
d) Choose the appropriate secret type.
e) Choose the appropriate encryption type.
f) Click **Save & Apply to Device**.

- Credentials

a) In the **Credentials** tab, enter local username and password details.
b) Choose the appropriate local password type.
c) Enter 802.1x username and password details.
d) Choose the appropriate 802.1x password type.
e) Enter the time in seconds after which the session should expire.
f) Enable local credentials and/or 802.1x credentials as required.
g) Click **Save & Apply to Device**.

- CDP Interface

a) In the **CDP Interface** tab, enable the CDP state, if required.
b) Click **Save & Apply to Device**.

Step 10 In the **Rogue AP** tab, check the **Rogue Detection** check box to enable rogue detection.

Step 11 In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

This field specifies the minimum RSSI value for which a Rogue AP should be reported. All Rogue APs with RSSI lower than what is configured will not be reported to controller.

Step 12 In the **Rogue Detection Transient Interval** field, enter the transient interval value.

This field indicates how long the Rogue AP should be seen before reporting the controller.

Step 13 In the **Rogue Detection Report Interval** field, enter the report interval value.

This field indicates the frequency (in seconds) of Rogue reports sent from AP to controller.

Step 14 Check the **Rogue Containment Automatic Rate Selection** check box to enable rogue containment automatic rate selection.

Here, the AP selects the best rate for the target Rogue, based on its RSSI.

Step 15 Check the **Auto Containment on FlexConnect Standalone** check box to enable the feature.

Here, the AP will continue containment in case it moves to FlexConnect standalone mode.

Step 16 Click **Save & Apply to Device**.

Configuring an AP Profile (CLI)

Follow the procedure given below to configure and AP profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** In an AP profile, the **EAP-FAST** is the default EAP type. **Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**description** *ap-profile-name* **Example:** `Device(config-ap-profile)# description "xyz ap profile"`	Adds a description for the ap profile.
Step 4	**ip dhcp fallback** **Example:** `Device(config-ap-profile)# ip dhcp fallback`	Configures DHCP fallback. **Note** DHCP fallback is enabled by default. So, if an AP is assigned a static IP address and unable to reach the controller, the AP falls back to the DHCP. To stop an AP from moving the static IP to DHCP, you must disable the DHCP fallback configuration in an AP join profile.
Step 5	**cdp** **Example:** `Device(config-ap-profile)# cdp`	Enables CDP for all Cisco APs.
Step 6	**end** **Example:**	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-ap-profile)# end`	
Step 7	**show ap profile name***profile-name* **detailed** **Example:** `Device# show ap profile name xyz-ap-profile detailed`	(Optional) Displays detailed information about an AP join profile.

Configuring User for AP Management (CLI)

Follow the procedure given below to configure a user for the AP management:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile default-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**mgmtuser username <username> password {0 | 8}** *<password>* **Example:** `Device(config-ap-profile)# mgmtuser username myusername password 0 12345678`	Specifies the AP management username and password for managing all of the access points configured to the controller. • **0**: Specifies an UNENCRYPTED password. • **8**: Specifies an AES encrypted password. **Note** While configuring an username, ensure that special characters are not used as it results in error with bad configuration.
Step 4	**end** **Example:** `Device(configure-ap-profile)# end`	Returns to privileged EXEC mode.

Setting a Private Configuration Key for Password Encryption

Follow the procedure given below to set a private configuration key for password encryption:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**key config-key password encrypt** key *<config-key>* **Example:** `Device(config)# key config-key password-encrypt 12345678`	Sets the password encryption keyword. Here, *config-key* refers to any key value with minimum 8 characters. **Note** The *config-key* value must not begin with the following special characters: !, #, and ;
Step 3	**password encryption aes** **Example:** `Device(config)# password encryption aes`	Enables the encrypted preshared key.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 On the **RF Profile** page, click **Add**.

Step 3 In the **General** tab, enter a name for the RF profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Choose the appropriate **Radio Band**.

Step 5 To enable the profile, set the status as **Enable**.

Step 6 Enter a **Description** for the RF profile.

Step 7 Click **Save & Apply to Device**.

Configuring an RF Profile (CLI)

Follow the procedure given below to configure an RF profile:

Before you begin

Ensure that you use the same RF profile name that you create here, when configuring the wireless RF tag too. If there is a mismatch in the RF profile name (for example, if the RF tag contains an RF profile that does not exist), the corresponding radios will not come up.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile and enters RF profile configuration mode. **Note** Use the **24ghz** command to configure the 802.11b parameters. Use the **5ghz** command to configure the 802.11a parameters. Use the **6ghz** command to configure the 802.11 6-GHz parameters.
Step 3	**default** **Example:** `Device(config-rf-profile)# default`	(Optional) Enables default parameters for the RF profile.
Step 4	**no shutdown** **Example:** `Device(config-rf-profile)# no shutdown`	Enables the RF profile on the device.
Step 5	**end** **Example:** `Device(config-rf-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 6	**show ap rf-profile summary** **Example:** `Device# show ap rf-profile summary`	(Optional) Displays the summary of the available RF profiles.
Step 7	**show ap rf-profile name** *rf-profile* **detail** **Example:** `Device# show ap rf-profile name rfprof24_1 detail`	(Optional) Displays detailed information about a particular RF profile.

Configuring a Site Tag (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page, click the **Site** tab.

Step 3 Click **Add** to view the **Add Site Tag** window.

Step 4 Enter a name and description for the site tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 5 Choose the required **AP Join Profile** to be attached to the site tag.

Step 6 Choose the required **Control Plane Name**.

Step 7 If required, enable the **Local Site**.

Disabling Local Site means that the site is remote and the deployment is FlexConnect mode.

Step 8 Click **Save & Apply to Device**.

Configuring a Site Tag (CLI)

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site rr-xyz-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	Configures a flex profile. **Note** You cannot remove the flex profile configuration from a site tag if local site is configured on the site tag.

	Command or Action	Purpose
		Note The **no local-site** command needs to be used to configure the Site Tag as Flexconnect, otherwise the Flex profile config does not take effect.
Step 4	**description** *site-tag-name* **Example:** `Device(config-site-tag)# description "default site tag"`	Adds a description for the site tag.
Step 5	**end** **Example:** `Device(config-site-tag)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless tag site summary** **Example:** `Device# show wireless tag site summary`	(Optional) Displays the number of site tags. **Note** To view detailed information about a site, use the **show wireless tag site detailed** *site-tag-name* command. **Note** The output of the **show wireless loadbalance tag affinity wncd** *wncd-instance-number* command displays default tag (site-tag) type, if both site tag and policy tag are not configured.

Enhanced Site Tag-Based Load Balancing

Feature History for Enhanced Site Tag-Based Load Balancing

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for Enhanced Site Tag-Based Load Balancing

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Enhanced Site Tag-Based Load Balancing	The Site Tag-based load balancing is available from Cisco IOS-XE Gibraltar 16.10.1 release. When the first AP from a site joins the controller, it takes the decision to load balance the entire site. However, this is done without knowing the site load. The enhancement to load balancing feature introduced in Cisco IOS-XE 17.10.1 specifies a site load to help with better load balancing.

Information About Enhanced Site Tag-Based Load Balancing

Load balancing of APs is done among session handling processes called Wireless Network Control Daemon (WNCD). The load balancer assigns APs to WNCDs based on site tags. The decision to load balance a site tag to a WNCD is taken when the first AP from that site tag joins the controller.

Prior to this enhancement, the controller had no indication about the size of the site. Therefore, the site size is not taken into consideration for this load balancing decision. The system works well only if the sites are of approximately equal size. However, in case where you have sites of disparate sizes, it is possible for some WNCDs to be more loaded than the others. This enhancement allows you to configure a site load, thus allowing the system to take better load balancing decisions.

The behavior of the load balancing feature in the controller reboot case is as follows:

- After you have configured the feature in one or more site tags and rebooted the controller, after the reboot, even before any APs join, the load balancing feature retains the site tags that are used actively in persistent memory and load balances them during bootup. The load balancing during bootup occurs in descending order of the configured site load.
- After you have configured the load balancing feature in a site tag with APs already joined, the load balancing remains unchanged unless all APs, including those not in the site tag, disconnects or the controller reboots.

Prerequisites for Enhanced Site Tag-Based Load Balancing

- You must have configured the site load.
- We recommended that you configure all the named sites with a load value.

Note The configured load is only an estimate. It will only be used for site load balancing. Specifically, it does not prevent APs, or clients from joining or associating.

Use Cases

To cater to a variety of use cases, the site load configuration is designed to be a load factor rather than an absolute number. Specifically, it need not be the number of APs in a site, although, for most practical purposes, the number of APs can be used as a good approximation of the load. The following are the two use cases:

- Sites with normal client density and roaming load. You can use AP count as a good approximate site load in these cases. Examples of such sites are cubicle areas in offices and hospitals.
- Sites with high client density and roaming load. For these, you can use a higher load configuration than the number of APs. For example, if the number of APs in such a site is 200, you can use a load factor of 300 or 400 to compensate for higher client load. Examples of such sites include stadiums, cafeterias, and conference floors.

Configuring Site Load (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-tag* **Example:** `Device(config)# wireless tag site area1`	Configures site tag and enters site tag configuration mode.
Step 3	**load** *load* **Example:** `Device(config-site-tag)# load 200`	Configures the site load. The *load* is the estimate of the relative load reserved for the site. Values range between 0 to 1000. The default value 0 means no load recommendation for the site.
Step 4	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode.

Verifying Enhanced Site Tag-Based Load Balancing Configuration

To view detailed information about a site, use the following command:

```
Device# show wireless tag site detailed area1
Site Tag Name        : area1
Description          :
-------------------------------------
AP Profile           : default-ap-profile
Local-site           : Yes
Image Download Profile: default
Fabric AP DHCP Broadcast : Disabled
```

```
Fabric Multicast Group IPv4 Address : 232.255.255.1
Site Load           : 200
```

To view the default site tag type for WNCD instances, use the following command:

```
Device# show wireless loadbalance tag affinity
Tag           Tag type    No of AP's Joined   Wncd Instance
-------------------------------------------------------------------------
area1         SITE TAG                  50         0
area2         SITE TAG                  50         0
area3         SITE TAG                  100        1
area4         SITE TAG                  150        2
```

Configuring Policy Tag (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **Policy**.

Step 2 Click **Add** to view the **Add Policy Tag** window.

Step 3 Enter a name and description for the policy tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Click **Add** to map WLAN and policy.

Step 5 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.

Step 6 Click **Save & Apply to Device**.

Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless tag policy** *policy-tag-name* **Example:**	Configures policy tag and enters policy tag configuration mode.

	Command or Action	Purpose
	`Device(config-policy-tag)# wireless tag policy default-policy-tag`	**Note** When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.
Step 4	**description** *description* **Example:** `Device(config-policy-tag)# description "default-policy-tag"`	Adds a description to a policy tag.
Step 5	**remote-lan** *name* **policy** *profile-policy-name* {**ext-module**| **port-id** } **Example:** `Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2`	Maps a remote-LAN profile to a policy profile.
Step 6	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1`	Maps a policy profile to a WLAN profile. **Note** Ensure that the WLAN profile is not used by any other profiles. If the AP uses the default profile, ensure that the **no central switching** command is configured on other profiles.
Step 7	**end** **Example:** `Device(config-policy-tag)# end`	Exits policy tag configuration mode, and returns to privileged EXEC mode.
Step 8	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	(Optional) Displays the configured policy tags. **Note** To view detailed information about a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Configuring Wireless RF Tag (GUI)

Procedure

Step 1 a) Choose **Configuration** > **Tags & Profiles** > **Tags** > **RF**.

Step 2 Click **Add** to view the **Add RF Tag** window.

Step 3 Enter a name and description for the RF tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Choose the required **5 GHz Band RF Profile**, **5 GHz Band RF Profile**, and **2.4 GHz Band RF Profile** to be associated with the RF tag.

Step 5 Click **Update & Apply to Device**.

Configuring Wireless RF Tag (CLI)

Follow the procedure given below to configure a wireless RF tag:

Before you begin

- You can use only two profiles (2.4-GHz and 5-GHz band RF profiles) in an RF tag.
- You can use only three profiles (2.4-GHz, 5-GHz and 6GHz band RF profiles) in an RF tag.
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag rf** *rf-tag* **Example:** `Device(config)# wireless tag rf rftag1`	Creates an RF tag and enters wireless RF tag configuration mode.
Step 3	**24ghz-rf-policy** *rf-policy* **Example:** `Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1`	Attaches an IEEE 802.11b RF policy to the RF tag. To configure a dot11a policy, use the **5ghz-rf-policy** command. To configure a 6GHz radio dot11 policy, use the **6ghz-rf-policy** command.
Step 4	**description** *policy-description* **Example:** `Device(config-wireless-rf-tag)# description Test`	Adds a description for the RF tag.
Step 5	**end** **Example:** `Device(config-wireless-rf-tag)# end`	Exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show wireless tag rf summary** **Example:** `Device# show wireless tag rf summary`	Displays the available RF tags.
Step 7	**show wireless tag rf detailed** *rf-tag* **Example:** `Device# show wireless tag rf detailed rftag1`	Displays detailed information of a particular RF tag.

Attaching a Policy Tag and Site Tag to an AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

The **All Access Points** section displays details of all the APs on your network.

Step 2 To edit the configuration details of an AP, select the row for that AP.

The **Edit AP** window is displayed.

Step 3 In the **General** tab and **Tags** section, specify the appropriate policy, site, RF tags, and radio profile that you created on the **Configuration** > **Tags & Profiles** > **Tags** page.

Step 4 Click **Update & Apply to Device**.

Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures a Cisco AP and enters AP profile configuration mode. **Note** The *mac-address* should be a wired mac address.

	Command or Action	Purpose
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag rr-xyz-site`	Maps a site tag to the AP.
Step 5	**rf-tag** *rf-tag-name* **Example:** `Device(config-ap-tag)# rf-tag rf-tag1`	Associates the RF tag.
Step 6	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 7	**show ap tag summary** **Example:** `Device# show ap tag summary`	(Optional) Displays AP details and the tags associated to it.
Step 8	**show ap name** <*ap-name*> **tag info** **Example:** `Device# show ap name ap-name tag info`	(Optional) Displays the AP name with tag information.
Step 9	**show ap name** <*ap-name*> **tag detail** **Example:** `Device# show ap name ap-name tag detail`	(Optional) Displays the AP name with tag details.

Configuring a Radio Profile

Information About Wireless Radio Profile

From Cisco IOS XE Bengaluru 17.6.1 onwards, you can configure radio profiles for the slots in access points (APs). In this release, you can configure radio profiles for beam-selection APs with the C-ANT9104 antenna and configure antenna count for Cisco Catalyst 9124AXI/D outdoor Access Points. You can configure the antenna beam-selection for the 5-GHz slots—slot 1 and slot 2. Because there is no default value for the beam-selection configuration, you must explicitly configure the beam selection mode for APs with the C-ANT9104 antenna.

The C-ANT9104 antenna-enabled Cisco Catalyst 9130AX Series APs have precise control over the antennae pattern. Therefore, a configuration knob in the controller in introduced to select the beam-steering direction

for the antennae. The C-ANT9104 antenna-enabled Cisco Catalyst 9130AX Series APs can operate on the following beam-steering modes:

- Wide beam
- Narrow beam
- Narrow beam with 10 degrees tilt
- Narrow beam with 20 degrees tilt

After creating the radio profile, you must link or attach the radio profile under the radio frequency (RF) tag configuration, so that the radio profile is applied to the APs.

Note When you add Cisco ANT9104 antennas to the wireless controller, RRM configuration is not supported for these antennas.

RRM features such as Dynamic Channel Assignment (DCA), Radio Transmit Power Control (TPC), Flexible Radio Assignment (FRA), and so on, are disabled on C-ANT9104 antenna-enabled Cisco Catalyst 9130 Series Access Points.

The sections in this topic describe the steps to configure radio profile, beam selection, antenna count, and how to link the radio profile to the slots.

Note Cisco Catalyst 9130 Series Access Points enabled with Cisco ANT9104 antenna are able to function with unsupported versions, for example, Cisco IOS XE Bengaluru 17.5.1.

If the AP that is enabled with Cisco ANT9104 antenna, has a software version that is earlier than Cisco IOS XE 17.6.1, the AP joins the controller but the AP will not be functional as the operation status of the radios will be down.

Configuring a Wireless Radio Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

Step 2 On the **Radio Profile** page, click **Add**.

Step 3 Enter a name for the Radio profile. Enter a description for the Radio profile.

Step 4 Choose the appropriate **Antenna Beam** selection.

Note The antenna beam selection is set to **Not Configured** if no settings are detected.

This option is to be configured for APs connected with the C-ANT9104 antenna.

Step 5 Enter the number in the **Number of antenna to be enabled** field.

Note The option is available for the Cisco Catalyst 9124AXE Outdoor Access Points.

Step 6 Click **Save & Apply to Device**.

Configuring a Radio Profile and Beam Selection

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile radio** *wireless-radio-profile* **Example:** `Device(config)# wireless profile radio wireless-radio-profile`	Configures the radio profile. Enters the wireless radio profile configuration mode.
Step 3	**antenna beam-selection** { **narrow tilt** {**10** | **20**} | **wide**} **Example:** `Device(config-wireless-radio-profile)# antenna beam-selection narrow tilt 10`	Configures the beam selection of the antenna under the new radio profile.

Configuring the Antenna Count in a Wireless Radio Profile

To configure the number of antennae for each slot, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile radio** *wireless-radio-profile* **Example:** `Device(config)# wireless profile radio wireless-radio-profile`	Configures the radio profile. Enters the wireless radio profile configuration mode.
Step 3	**antenna count** *<0 - 8>* **Example:** `Device(config-wireless-radio-profile)# antenna count 4`	Configures the number of antennas to be enabled under the new radio profile.

Configuring a Slot Per Radio in the RF Tag Profile

It is mandatory to link radio profiles under an RF tag for the radio profile configurations to get applied. To configure a radio profile for each slot in an RF tag profile, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag rf** *wireless-rf-tagname* **Example:** `Device(config)# wireless tag rf wireless-rf-tagname`	Configures the RF tag. Enters the wireless RF tag configuration mode.
Step 3	**dot11**{ **24ghz slot0** | **5ghz** { **slot1** | **slot2**} **radio-profile** *radio-profile-name*} **Example:** `Device(config-wireless-rf-tag)# dot11 5ghz slot1 radio-profile wireless-radio-profile`	Configures the 802.11a/802.11b radio profile.

Verifying a Radio Profile

To view the summary of all the configured radio profiles, use the following command:

```
Device# show wireless profile radio summary

Number of radio-profiles: 3

Antenna Profile Name             Description
------------------------------------------------------------------------
radio-profile-1                  Custom profile for Slot1
antenna-ewlc                     Add description
default_radio_profile            Preconfigured default radio profile
```

To view detailed information about the parameters configured for a radio profile, use the following command:

```
Device# show wireless profile radio detailed radio-profile-name
Radio Profile name                              : radio-profile-1
Description                                     : Custom profile for slot1
Beam-Selection                                  : Wide beam
```

To view radio profile and RF tag information, use the following command:

```
Device # show ap name Cisco-AP tag info
AP Name            : Cisco-AP
AP Mac             : 04xx.40xx.XXXX

Applied Tags :
-----------------------------------------
  Tag Type             Tag Name
  -----------------------------------------
```

```
  RF Tag               test-rf
  Site Tag             default-site-tag
  Policy Tag           default-policy-tag

Tag/Profile Type Misconfigured
----------------------------------------
RF Tag No
Policy Tag No
Site Tag No
Flex profile No
AP join profile No
2.4GHz Rf Profile No
5 GHz Rf Profile No
5 GHz Slot1 Radio Profile NO
5 GHz Slot2 Radio Profile Yes

Resolved Tags :
----------------------------------------
Tag Source         : Static

  Tag Type             Tag Name
  ----------------------------------------
  RF Tag               test-rf
  Site Tag             default-site-tag
  Policy Tag           default-policy-tag
```

To display beam selection and the number of antennas, run the following commands:

```
Device# show wireless profile radio detailed radio-profile-1
Radio Profile name : radio-profile-1
Description        : Custom profile for slot1
Beam-Selection     : Wide beam
```

```
Device# show ap name cisco-ap config slot 1 | section 11n
802.11n Antennas
      Number of Antennas selected               : 2
      Supported Antenna  modes                  : 1x1 2x2 4x4
      Antenna port mapping                      : AB
      SIA Status                                : Not Present
```

```
Device# show ap name cisco-ap config slot 1 | include beam
Beam Selection : Narrow from centre 20
```

AP Filter

Introduction to AP Filter

The introduction of tags in the new configuration model in the Cisco Catalyst 9800 Series Wireless Controller has created multiple sources for tags to be associated with access points (APs). Tag sources can be static configuration, AP filter engine, per-AP PNP, or default tag sources. In addition to this, the precedence of the tags also plays an important role. The AP filter feature addresses these challenges in a seamless and intuitive manner.

AP filters are similar to the access control lists (ACLs) used in the controller and are applied at the global level. You can add AP names as filters, and other attributes can be added as required. Add the filter criteria as part of the discovery requests.

The AP Filter feature organizes tag sources with the right priority, based on the configuration.

You cannot disable the AP filter feature. However, the relative priority of a tag source can be configured using **ap filter-priority** *priority filter-name* command.

Note You can configure tag names at the PnP server (similar to the Flex group and AP group) and the AP stores and send the tag name as part of discovery and join requests.

Set Tag Priority (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Tag Source**.

Step 2 Drag and Drop the Tag Sources to change priorities.

Set Tag Priority

Multiple tag sources might result in ambiguity for network administrators. To address this, you can define priority for tags. When an AP joins the controller, the tags are picked based on priority. If precedence is not set, the defaults are used.

Use the following procedure to set tag priority:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap tag-source-priority** *source-priority* **source {filter | pnp}** **Example:** `Device(config)# ap tag-source-priority 2 source pnp`	Configures AP tag source priority. **Note** It is not mandatory to configure AP filter. It comes with default priorities for Static, Filter, and PnP.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 4	**ap tag-sources revalidate** **Example:**	Revalidates AP tag sources. The priorities become active only after this command is run.

	Command or Action	Purpose
	`Device# ap tag-sources revalidate`	**Note** If you change the priorities for Filter and PnP, and want to evaluate them, run the **revalidate** command.

Create an AP Filter (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Filter**.

Step 2 Click **Add**.

Step 3 In the **Associate Tags to AP** dialog box which is displayed, enter the **Rule Name**, the **AP name regex** and the **Priority**. Optionally, you can also choose the policy tag from the **Policy Tag Name** drop-down list, the site tag from the **Site Tag Name** drop-down list and the RF tag from the **RF Tag Name** drop-down list.

Step 4 Click **Apply to Device**.

Create an AP Filter (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap filter name** *filter_name* **Example:** `Device(config)# ap filter filter-1`	Configures an AP filter.
Step 3	**ap name-regex** *regular-expression* **Example:** `Device(config-ap-filter)# ap name-regex testany`	Configures the AP filter based on regular expression. For example, if you have named an AP as **ap-lab-12**, then you can configure the filter with a regular expression, such as **ap-lab-\d+** , to match the AP name.
Step 4	**tag policy** *policy-tag* **Example:** `Device(config-ap-filter)# tag policy pol-tag1`	Configures a policy tag for this filter.

	Command or Action	Purpose
Step 5	**tag rf** *rf-tag* **Example:** `Device(config-ap-filter)# tag rf rf-tag1`	Configures an RF tag for this filter.
Step 6	**tag site** *site-tag* **Example:** `Device(config-ap-filter)# tag site site1`	Configures a site tag for this filter.
Step 7	**end** **Example:** `Device(config-ap-filter)# end`	Exits configuration mode and returns to privileged EXEC mode.

Set Up and Update Filter Priority (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Filter**.

Step 2
a) If you want to setup a new AP filter, then click **Add**. In the **Associate Tags to AP** dialog box which is displayed, enter the **Rule Name**, the **AP name regex** and the **Priority**. Optionally, you can also select the **Policy Tag Name**, the **Site Tag Name** and the **RF Tag Name**. Click **Apply to Device**.
b) If you want to update the priority of an existing AP filter, click on the Filter and in the **Edit Tags** dialog box and change the **Priority**. In case the Filter is Inactive, no priority can be set to it. Click **Update and Apply to Device**.

Set Up and Update Filter Priority

Follow the procedure given below to set and update filter priority:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap filter priority** *priority* **filter-name** *filter-name* **Example:** `Device(config)# ap filter priority 10 filter-name test1`	Configure AP filter priority. Valid values range from 0 to 1023; 0 is the highest priority. **Note** A filter without a priority is not active. Similarly, you cannot set a filter priority without a filter.

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config-ap)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verify AP Filter Configuration

The following **show** commands are used to display tag sources and filters, and their priorities.

To view the tag source priorities, use the following command:

```
Device# show ap tag sources

Priority Tag source
--------------------------------
0 Static
1 Filter
2 AP
3 Default
```

To view the available filters, use the following command:

```
Device# show ap filter all

Filter Name             regex             Policy Tag               RF Tag              Site
 Tag
------------------------------------------------------------------------------------------------
first                    abcd              pol-tag1                 rf-tag1
site-tag1
test1                   testany                                                        site1

filter1                  testany
```

To view the list of active filters, use the following command:

```
Device# show ap filters active

Priority   Filter Name       regex          Policy Tag              RF Tag
Site Tag
------------------------------------------------------------------------------------------------------
10         test1             testany
site1
```

To view the source of an AP tag, use the following command:

```
Device# show ap tag summary

Number of APs: 4

AP Name          AP Mac         Site Tag Name    Policy Tag Name    RF Tag Name
Misconfigured Tag Source
-----------------------------------------------------------------------------------------------
AP002A.1034.CA78 002a.1034.ca78 named-site-tag   named-policy-tag   named-rf-tag   No Filter

AP00A2.891C.2480 00a2.891c.2480 named-site-tag   named-policy-tag   named-rf-tag   No Filter

AP58AC.78DE.9946 58ac.78de.9946 default-site-tag default-policy-tag default-rf-tag No AP
AP0081.C4F4.1F34 0081.c4f4.1f34 default-site-tag default-policy-tag default-rf-tag No Default
```

Configuring Access Point for Location Configuration

Information About Location Configuration

During location configuration, you can perform the following:

- Configure a site or location for an AP.
- Configure a set of tags for this location.
- Add APs to this location.

Any location comprises of the following components:

- A set of unique tags, one for each kind, namely: Policy, RF and Site.
- A set of ethernet MAC addresses that applies to the tags.

This feature works in conjunction with the existing tag resolution scheme. The location is considered as a new tag source to the existing system. Similar, to the static tag source.

Prerequisite for Location Configuration

If you configure an access point in one location, you cannot configure the same access point in another location.

Configuring a Location for an Access Point (GUI)

Before you begin

Note When you create local and remote sites in the Basic Setup workflow, corresponding policies and tags are created in the backend. These tags and policies that are created in the Basic Setup cannot be modified using the Advanced workflow, and vice versa.

Procedure

Step 1 Choose **Configuration** > **Wireless Setup** > **Basic**.

Step 2 On the **Basic Wireless Setup** page, click **Add**.

Step 3 In the **General** tab, enter a name and description for the location.

Step 4 Set the **Location Type** as either *Local* or *Flex*.

Step 5 Use the slider to set **Client Density** as *Low*, *Typical* or *High*.

Step 6 Click **Apply**.

Configuring a Location for an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap location name** *location_name* **Example:** `Device(config)# ap location name location1`	Configures a location for an access point. Run the **no** form of this command to remove location for an access point.

Step 3	**tag** {**policy** *policy_name*| **rf** *rf_name* | **site** **site_name**}
	Example:
	`Device(config-ap-location)# tag policy policy_tag`
	`Device(config-ap-location)# tag rf rf_tag`
	`Device(config-ap-location)# tag site site_tag`
		Configures tags for the location.

Step 4	**location** *description* **Example:** `Device(config-ap-location)# location description`	Adds description to the location.
Step 5	**end** **Example:** `Device(config-ap-location)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Adding an Access Point to the Location (GUI)

Note When the tag source is not set to location, the AP count and AP location tagging will not be correctly reflected on the web UI. To change static tag source on the AP, run the **no ap** *ap-mac* command on the controller to change AP tag source to default (which is location).

Procedure

Step 1 Choose **Configuration** > **Wireless Setup** > **Basic**.

Step 2 On the **Basic Wireless Setup** page, click **Add** to configure the following:

- General
- Wireless Networks
- AP Provisioning

Step 3 In the **AP Provisioning** tab and **Add/Select APs** section, enter the AP MAC address and click the right arrow to add the AP to the associated list. The MAC address can be either in *xx:xx:xx:xx:xx:xx*, *xx-xx-xx-xx-xx-xx*, or *xxxx.xxxx.xxxx* format.

You can also add a CSV file from your system. Ensure that the CSV has the MAC Address column.

Step 4 Use the search option in the **Available AP List** to select the APs from the Selected AP list and click the right arrow to add the AP to the associated list.

Step 5 Click **Apply**.

Adding an Access Point to the Location (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap location name** *location_name* **Example:** `Device(config)# ap location name location1`	Configures a location for an access point.
Step 3	**ap-eth-mac** *ap_ethernet_mac* **Example:** `Device(config-ap-location)# ap-eth-mac 188b.9dbe.6eac`	Adds an access point to the location.
Step 4	**end** **Example:** `Device(config-ap-location)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. **Note** After adding an AP to a location, the AP may reset automatically to get the new configuration

Configuring SNMP in Location Configuration

SNMP MIB

The SNMP MIB provides information on a set of managed objects that represent logical and physical entities, and relationships between them.

Table 2: MIB Objects and Notes

MIB Objects	Notes
cLApLocationName	Provides the name of the AP location.
cLApLocationPolicyTag	Provides the policy tag configured on the location.
cLApLocationSitetag	Provides the site tag configured on the location.
cLApLocationRfTag	Provides the RF tag configured on the location.
cLAssociatedApsApMac	Provides the configured APs on the location.

Verifying Location Configuration

To view the summary of AP location configuration, use the following command:

```
Device# show ap location summary

Location Name    Description     Policy Tag           RF Tag           Site Tag
-------------------------------------------------------------------------------------------------
first            first floor     default-policy-tag   default-rf-tag   default-site-tag
second           second floor    default-policy-tag   default-rf-tag   default-site-tag
```

To view the AP location configuration details for a specific location, use the following command:

```
Device# show ap location details first

Location Name.....................: first
Location description..............: first floor
Policy tag........................: default-policy-tag
Site tag..........................: default-site-tag
RF tag............................: default-rf-tag

Configured list of APs
005b.3400.0af0
005b.3400.0bf0
```

To view the AP tag summary, use the following command:

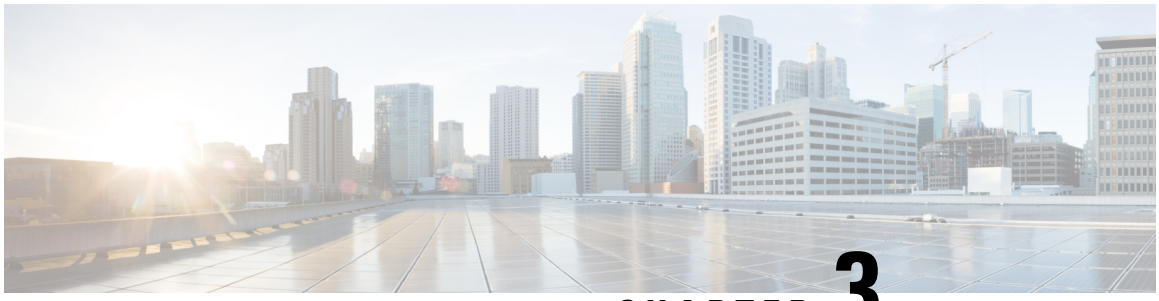
```
Device# show ap tag summary

Number of APs: 4
AP Name      AP Mac           Site Tag Name      Policy Tag Name      RF Tag Name
Misconfigured  Tag Source
-----------------------------------------------------------------------------------------------------------------
Asim_5-1     005b.3400.02f0   default-site-tag   default-policy-tag   default-rf-tag   Yes
            Filter
Asim_5-2     005b.3400.03f0   default-site-tag   default-policy-tag   default-rf-tag   No
            Default
Asim_5-9     005b.3400.0af0   default-site-tag   default-policy-tag   default-rf-tag   No
```

```
            Location
Asim_5-10    005b.3400.0bf0   default-site-tag   default-policy-tag   default-rf-tag   No
            Location
```

Verifying Location Statistics

To view the AP location statistics, use the following command:

```
Device# show ap location stats

Location name    APs joined     Clients joined     Clients on 11a     Clients on 11b
-------------------------------------------------------------------------------------------------
first             2             0                   3                  4
second            0             0                   0                  0
```



CHAPTER 3

Wireless Management Interface

- Information About Wireless Management Interface, on page 47
- Recommendations for Wireless Management Interface, on page 48
- Configuring your Controller with Wireless Management Interface (CLI), on page 49
- Verifying Wireless Management Interface Settings, on page 51
- Information About Network Address Translation (NAT), on page 52
- Information About CAPWAP Discovery, on page 52
- Configuring Wireless Management Interface with a NAT Public IP (CLI), on page 53
- Configuring CAPWAP Discovery to Respond Only with Public or Private IP (CLI), on page 54
- Verifying NAT Settings, on page 55

Information About Wireless Management Interface

The Wireless Management Interface (WMI) is the mandatory Layer 3 interface on the Cisco Catalyst 9800 Wireless Controller. It is used for all communications between the controller and access points. Also, it is used for all CAPWAP or inter-controller mobility messaging and tunneling traffic.

WMI is also the default interface for in-band management and connectivity to enterprise services, such as, AAA, syslog, SNMP, and so on. You can use the WMI IP address to remotely connect to the device using SSH or Telnet (or) access the Graphical User Interface (GUI) using HTTP or HTTPs by entering the wireless management interface IP address of the controller in the address field of your browser.

The Cisco Catalyst 9800 Series Wireless Controller should be able to use Ethernet Service Port (SP) (Management Interface VRF/GigabitEthernet 0) for the below management/control plane protocols from release 17.6.1 onwards:

- SNMP
- RADIUS (both for user authentication to the box and wireless client authorization)
- TACACS
- Syslog
- NTP
- SSH/NETCONF/HTTPS
- NetFlow

Recommendations for Wireless Management Interface

The Wireless Management Interface is a Layer 3 interface, which can be configured only with a single IP address (IPv4 or IPv6) or using a dual-stack configuration.

It is always recommended to use a wireless management VLAN and configure WMI as a Switched VLAN Interface (SVI). If the uplink port or port-channel to the next-hop switch is configured as a dot1q trunk, the wireless management VLAN would be one of the allowed tagged VLAN on the trunk.

The recommendation is true, independent of the deployment mode of APs (local, FlexConnect, or SDA) with the following exceptions:

- The WMI is configured as an L3 port for Cisco Catalyst 9800 Wireless Controller deployed in a Public Cloud environment.
- The WMI is configured as a loopback interface for embedded wireless controller in Cisco Catalyst 9000 switches.

It is always recommended to statically assign IPv6 address in WMI and not configure using the **ipv6 auto-config** command.

Note The **ipv6 auto-config** command is not supported.

Note You can use only one AP manager interface on Cisco Catalyst 9800 Wireless Controller called the WMI to terminate CAPWAP traffic.

Note There is only one Wireless Management Interface (WMI) on the controller.

Note Layer 3 interface is not supported in Cisco Catalyst 9800-CL Cloud Wireless Controller Guest anchor scenarios.

Instead, it is recommended to use the Layer 2 interfaces and SVI for WMI.

It is recommended to use Layer 3 interface for Public cloud deployments only and not for on-premise as it poses some limitations.

The following are the sample Layer 3 and Layer 2 interface configurations:

Layer 3 interface configuration:

```
interface GigabitEthernet2
no switchport
ip address <ip_address> <mask>
negotiation auto
no mop enabled
no mop sysid
end
```

Layer 2 interface configuration:

```
interface GigabitEthernet2
switchport trunk allowed vlan 25,169,504
switchport mode trunk
negotiation auto
no mop enabled
no mop sysid
end
```

Note To change the WMI interface when RMI is configured, perform the following:

1. Unconfigure the RMI, save the changes using the **write memory** command, and reload the controller.
2. Change the WMI interface.
3. Reconfigure the RMI in the same interface as WMI, save the changes using the **write memory** command, and reload the controller.

Configuring your Controller with Wireless Management Interface (CLI)

You can configure the Wireless Management interface using CLI by directly accessing the physical console (for the Cisco Catalyst 9800 appliances) (or) using the virtual console in case of the Cisco Catalyst 9800-CL Cloud Wireless Controller.

Note The example assumes that:

- You have a Cisco Catalyst 9800-CL Cloud Wireless Controller and the GigabitEthernet 2 is connected to a trunk interface on the uplink switch.
- You want to configure multiple VLANs and dedicate one for Wireless Management interface.

Procedure

Step 1 Access the CLI using VGA or monitor console from the hypervisor of your choice.

Step 2 Terminate the configuration wizard.

```
Would you like to enter the initial configuration dialog? [yes/no]:
no
Would you like to terminate autoinstall? [yes]:
yes
```

Step 3 Enter the configuration mode and add the login credentials using the following command:

```
Device# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# username <name> privilege 15 password <yourpwd>
```

Step 4 (Optional) Set a hostname.

```
Device(config)# hostname C9800
```

Step 5 Configure the VLAN for wireless management interface:

```
Device(config)# vlan 201
Device(config-vlan)# name wireless_management
```

Step 6 Configure the L3 SVI for wireless management interface:

```
Device(config)# int vlan 201
Device(config-if)# description wireless-management-interface
Device(config-if)# ip address 172.16.201.21 255.255.255.192
Device(config-if)# no shutdown
```

Step 7 Configure the interface GigabitEthernet 2 as trunk and allow the wireless management VLAN:

```
Device(config-if)# interface GigabitEthernet2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport trunk allowed vlan 201,210,211
Device(config-if)# shut
Device(config-if)# no shut
```

Note VLANs 210 and 211 are added to the trunk to carry client traffic.

Step 8 Configure a default route (or a more specific route) to reach the device:

```
Device(config-if)# ip route 0.0.0.0 0.0.0.0 172.16.201.1
```

At this point you can use SSH or Telnet, or GUI to access the device, or use the Cisco Catalyst Center or Cisco Prime to continue with the DAY 0 configuration.

Verifying Wireless Management Interface Settings

To verify if the Layer 3 interface is configured correctly, use the following command:

```
Device# show run int vlan 201

Building configuration...

Current configuration : 128 bytes
!
interface Vlan201
 description wireless-management-interface
 ip address 172.16.201.21 255.255.255.0
 no mop enabled
 no mop sysid
end
```

To verify if the wireless management VLAN is active on the uplink to the network, use the following command. In this case the uplink is a trunk interface, so the VLAN needs to be active and forwarding state.

```
Device# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi2         on               802.1q         trunking      1
.....
Port        Vlans allowed on trunk
Gi2         201,210-211
.....
Port        Vlans allowed and active in management domain
Gi2         201,210-211
....
Port        Vlans in spanning tree forwarding state and not pruned
Gi2         201,210-211
....
```

To verify if the wireless management interface is up, use the following command:

```
Device# show ip int brief | i Vlan201
Vlan201   172.16.201.21  YES NVRAM  up  up
```

To verify if the selected interface has been configured as wireless management, use the following command:

```
Device# show wireless interface summary

Wireless Interface Summary

Interface Name Interface Type VLAN ID IP Address     IP Netmask   NAT-IP Address MAC Address
-----------------------------------------------------------------------------------------------
Vlan201      Management      201   172.16.201.21  255.255.255.0  0.0.0.0     001e.e51c.a7ff
```

Information About Network Address Translation (NAT)

NAT enables private IP networks that use non-registered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks. Before packets are forwarded onto another network, NAT translates the private (not globally unique) addresses from the internal network into public addresses. NAT can be configured to advertise to the outside world only few addresses for the entire internal network. This ability provides more security by effectively hiding the private network details.

If you want to deploy your Cisco Catalyst 9800 Wireless Controller on a private network and make it reachable from internet, you need to have the controller behind a router, firewall, or other gateway device that uses one-to-one mapping Network Address Translation (NAT).

To do so, perform the following:

- Configure the NAT device with 1:1 static mapping of the Wireless Management interface IP address (private IP) to a unique external (public) IP address configured on the NAT device.
- Enable the NAT feature on the Wireless Controller and specify its external public IP address. This public IP is used in the discovery responses to APs, so that the APs can then send CAPWAP packets to the right destination.
- Make sure that the external APs discover the public IP of the controller using DHCP, DNS, or PnP.

Note You need not enable NAT if the Cisco Catalyst 9800 Wireless Controller is deployed with a public address. Instead you will need to configure the public IP directly on the Wireless Management Interface (WMI).

Information About CAPWAP Discovery

In a CAPWAP environment, a lightweight access point discovers a wireless controller by using CAPWAP discovery mechanisms, and then sends a CAPWAP join request to the controller. The controller sends a CAPWAP join response to the access point that allows the access point to join the controller.

If the wireless controller is behind a NAT device, the controller responds to the discovery response in the following ways:

- Using the public IP.
- Using the private IP.
- Using public and private IP.

The Public IP needs to be mapped to the controller's Private IP using static 1:1 NAT configuration on the router or firewall performing the NAT translation.

If your wireless controller manages only Access Points reachable through the public internet (external APs), you need to configure the controller so it responds with only the Public IP in the discovery response.

If your wireless controller manages both internal and external APs, you need to configure the controller so it responds with both Public and Private IPs in the discovery response.

Note In NAT deployments, the APs running internally and externally must use different AP join profiles with CAPWAP Discovery Private and Public enabled separately. This behaviour was introduced from the 17.9.5 release and applies to APs upgraded to Cisco IOS XE 17.12.x and later.

Configuring Wireless Management Interface with a NAT Public IP (CLI)

The first step is to configure the controller to use the public NAT IP (this is the public IP that has been configured on the NAT device to statically map 1:1 the WMI's private IP address).

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless management interface** *interface-type interface-number* **Example:** `Device(config)# wireless management interface vlan 20`	Defines the management interface. Here, • *interface-type*—Refers to the VLAN, Gigabit, or loopback types. • *interface-number*—Is the interface number.
Step 3	**public-ip** *external-public-ip* **Example:** `Device(config-mgmt-interface)# public-ip 2.2.2.2`	Defines the external NAT or Public IP.
Step 4	**end** **Example:** `Device(config-mgmt-interface)# end`	Returns to privileged EXEC mode.

Configuring CAPWAP Discovery to Respond Only with Public or Private IP (CLI)

Note By default, if the wireless management interface is configured with a public IP, the controller responds with both Public and Private IP in the CAPWAP discovery response.

The setting to determine the IP (private or public) to include in the discovery response is available in the AP Join profile.

Configuring the Controller to Respond only with a Public IP (CLI)

Configure the Controller to respond only with a Public IP using commands.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**no capwap-discovery private** **Example:** `Device(config-ap-profile)# no capwap-discovery private`	Instructs the controller to not respond with the internal IP. Enables AP to join the controller over Public IP only.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

Configuring the Controller to Respond only with a Private IP (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**no capwap-discovery public** **Example:** `Device(config-ap-profile)# no capwap-discovery public`	Instructs the controller to not respond with the public IP. Enables AP to join the controller over private IP only.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

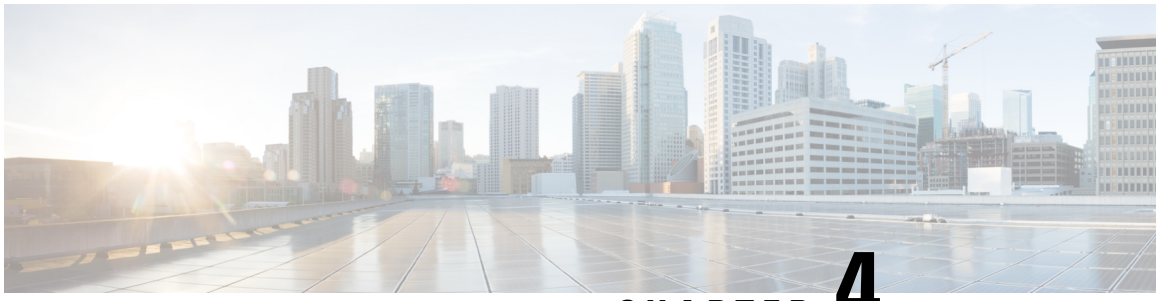
Verifying NAT Settings

Verify NAT Settings using commands.

```
Device# show wireless interface summary

Wireless Interface Summary

Interface Name Interface Type VLAN ID IP Address     IP Netmask     NAT-IP Address   MAC
Address
-----------------------------------------------------------------------------------------------
Vlan20         Management     20      10.58.20.25    255.255.255.0  2.2.2.2    001e.4963.1cff
```

To verify the settings in the AP join profile, use the following command

```
Device# show run | b ap profile

ap profile default-ap-profile
 no capwap-discovery private
 description "default ap profile"
...
```



CHAPTER 4

BIOS Protection

- BIOS Protection on the Controller, on page 57
- BIOS or ROMMON Upgrade with BIOS Protection, on page 57
- Upgrading BIOS, on page 58

BIOS Protection on the Controller

BIOS Protection enables you to protect and securely update BIOS flash for Intel-based platforms. If BIOS Protection is not used, the flash utility that stores the BIOS for an Intel platform is not write-protected. As a result, when BIOS updates are applied, malicious code also makes its way through.

By default, BIOS Protection works by bundling the flash containing the BIOS image, and by accepting updates only through the BIOS capsules that enable writing on the BIOS Flash.

BIOS or ROMMON Upgrade with BIOS Protection

To upgrade BIOS or ROMMON use the BIOS Protection feature as follows:

1. The new BIOS image capsule bundled together with the ROMMON binary is inserted into the media of the Cisco device by the ROMMON upgrade scripts.
2. The Cisco device is then reset for the new BIOS/ROMMON upgrade to take place.
3. On reset, the original BIOS detects the updated capsule and determines if the updated BIOS is available.
4. The original BIOS then verifies the digital signature of the BIOS capsule. If the signature is valid, the original BIOS will remove write-protection from the flash utility and update the SPI flash with the new BIOS image. If the BIOS capsule is invalid, the SPI flash is not updated.
5. After the new BIOS/ROMMON image is written to the SPI flash, the required regions of the SPI flash are once again write-protected.
6. After the card is reset, the updated BIOS is rebooted.
7. The capsule is deleted by BIOS.

Upgrading BIOS

Procedure

Use the **upgrade rom-monitor filename** command to update the BIOS capsule.

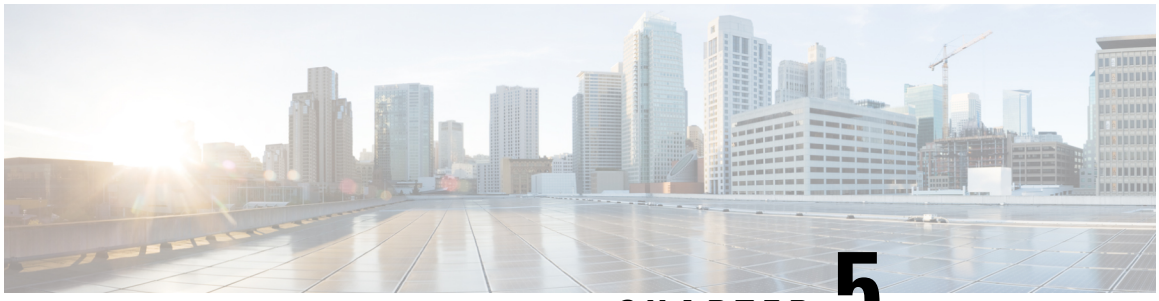
Example:

```
upgrade rom-monitor filename bootflash:capsule.pkg <slot>
```

Example

The following example shows you how to verify a BIOS Protection upgrade:

```
Device# upgrade rom-monitor filename bootflash:qwlc-rommon-capsule-p106.pkg all
Verifying the code signature of the ROMMON package...
Chassis model AIR-CT5540-K9 has a single rom-monitor.

Upgrade rom-monitor

Target copying rom-monitor image file

Secure update of the ROMMON image will occur after a reload.

8388608+0 records in
8388608+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 11.9671 s, 701 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 0.414327 s, 316 kB/s
Copying ROMMON environment
8388608+0 records in
8388608+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 31.1199 s, 270 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 2.44015 s, 53.7 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 2.43394 s, 53.9 kB/s
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.
Device#reload
```



CHAPTER 5

Smart Licensing Using Policy

- Introduction to Smart Licensing Using Policy, on page 59
- Information About Smart Licensing Using Policy, on page 60
- How to Configure Smart Licensing Using Policy: Workflows by Topology , on page 86
- Migrating to Smart Licensing Using Policy, on page 100
- Task Library for Smart Licensing Using Policy, on page 121
- Troubleshooting Smart Licensing Using Policy, on page 164
- Additional References for Smart Licensing Using Policy, on page 176
- Feature History for Smart Licensing Using Policy, on page 176

Introduction to Smart Licensing Using Policy

Smart Licensing Using Policy is an enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use.

Smart Licensing Using Policy is supported starting with Cisco IOS XE Amsterdam 17.3.2a.

The primary benefits of this enhanced licensing model are:

- Seamless day-0 operations

  After a license is ordered, no preliminary steps, such as registration or generation of keys etc., are required unless you use an export-controlled or enforced license. There are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers and product features can be configured on the device right-away.

- Consistency in Cisco IOS XE

  Campus and industrial ethernet switching, routing, and wireless devices that run Cisco IOS XE software, have a uniform licensing experience.

- Visibility and manageability

  Tools, telemetry and product tagging, to know what is in-use.

- Flexible, time series reporting to remain compliant

  Easy reporting options are available, whether you are directly or indirectly connected to Cisco Smart Software Manager (CSSM), or in an air-gapped network.

This document provides conceptual, configuration, and troubleshooting information for Smart Licensing Using Policy on Cisco Catalyst Wireless Controllers.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Information About Smart Licensing Using Policy

This section provides conceptual information about Smart Licensing Using Policy, supported products, an overview of each supported topology, and explains how Smart Licensing Using Policy interacts, with other features.

Overview

Smart Licensing Using Policy is a software license management solution that provides a seamless experience with the various aspects of licensing.

- Purchase licenses: Purchase licenses through the existing channels and use the Cisco Smart Software Manager (CSSM) portal to view product instances and licenses.

Note For new hardware or software orders, Cisco simplifies the implementation of Smart Licensing Using Policy, by factory-installing the following (terms are explained in the #unique_88 section further below):

- A custom policy, if available.
- A trust code, which ensures authenticity of data sent to CSSM. This is installed starting with Cisco IOS XE Cupertino 17.7.1. This trust code cannot be used to *communicate* with CSSM.

- Use: All licenses on Cisco Catalyst Wireless Controllers are unenforced. This means that you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.
- Report license usage to CSSM: Multiple options are available for license usage reporting. You can use Cisco Smart Licensing Utility (CSLU), or report usage information directly to CSSM. For air-gapped networks, a provision for offline reporting where you download usage information and upload it to CSSM, is also available. The usage report is in plain text XML format. See: #unique_89.
- Reconcile: For situations where delta billing applies (purchased versus consumed).

Supported Products

This section provides information about the Cisco IOS-XE product instances that support Smart Licensing Using Policy. All models (Product IDs or PIDs) in a product series are supported – unless indicated otherwise.

Table 3: Supported Product Instances: Cisco Catalyst Wireless Controllers

Cisco Catalyst Wireless Controllers	When Support for Smart Licensing Using Policy was Introduced
Cisco Catalyst 9800-40 Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800-L Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800-CL Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800 embedded Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a
Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points (EWC-AP)	Cisco IOS XE Amsterdam 17.3.2a

Architecture

This section explains the various components that can be part of your implementation of Smart Licensing Using Policy. One or more components make up a topology.

Product Instance

A product instance is a single instance of a Cisco product, identified by a Unique Device Identifier (UDI).

A product instance records and reports license usage (RUM reports), and provides alerts and system messages about overdue reports, communication failures, etc. RUM reports and usage data are securely stored in the product instance.

Throughout this document, the term *product instance* refers to all supported physical and virtual product instances - unless noted otherwise. For information about the product instances that are within the scope of this document, see #unique_93.

CSLU

Cisco Smart License Utility (CSLU) is a Windows-based reporting utility that provides aggregate licensing workflows. This utility performs the following key functions:

- Provides options relating to how workflows are triggered. The workflows can be triggered by CSLU or by a product instance.
- Collects usage reports from one or more product instances and uploads these usage reports to the corresponding Smart Account or Virtual Account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and sent back to the product instance.
- Sends authorization code requests to CSSM and receives authorization codes from CSSM, if applicable.

CSLU can be part of your implementation in the following ways:

- Install the windows application, to use CSLU as a standalone tool that is connected to CSSM.
- Install the windows application, to use CSLU as a standalone tool that is disconnected from CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited to air-gapped networks.

- Embedded (by Cisco) in a controller such as Cisco Catalyst Center.
- Deploy CSLU on a machine (laptop or desktop) running Linux.

CSLU supports Windows 10 and Linux operating systems. For release notes and to download the latest version, click *Smart Licensing Utility* on the Software Download page

CSSM

Cisco Smart Software Manager (CSSM) is a portal that enables you to manage all your Cisco software licenses from a centralized location. CSSM helps you manage current requirements and review usage trends to plan for future license requirements.

You can access the CSSM Web UI at https://software.cisco.com. Under the **License** tab, click the **Smart Software Licensing** link.

See the #unique_96 section to know about the different ways in which you can connect to CSSM

In CSSM you can:

- Create, manage, or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove, or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.

Controller

A management application or service that manages multiple product instances.

Note Throughout this chapter, and in the context of Smart Licensing Using Policy, the term "controller" or "Controller" always means a management application or service that manages a product instance. The term is not used to refer to Cisco Catalyst Wireless Controllers, which are *product instances*.

On Cisco Catalyst Wireless Controllers, Cisco Catalyst Center is the supported controller. Information about the controller, product instances that support the controller, and minimum required software versions on the controller and on the product instance is provided below:

Table 4: Support Information for Controller: Cisco Catalyst Center

Minimum Required Cisco Catalyst Center Version for Smart Licensing Using Policy[1]	Minimum Required Cisco IOS XE Version[2]	Supported Product Instances
Cisco Catalyst Center Release 2.2.2	Cisco IOS XE Amsterdam 17.3.2a	• Cisco Catalyst 9800-40 Wireless Controller • Cisco Catalyst 9800-80 Wireless Controller • Cisco Catalyst 9800-L Wireless Controller • Cisco Catalyst 9800-CL Wireless Controller • Cisco Catalyst 9800 embedded Wireless Controller • Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points (EWC-AP)

1 The minimum required software version on the controller. This means support continues on all subsequent releases - unless noted otherwise

2 The minimum required software version on the product instance. This means support continues on all subsequent releases - unless noted otherwise.

For more information about Cisco Catalyst Center, see the support page at: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html.

SSM On-Prem

Smart Software Manager On-Prem (SSM On-Prem) is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM.

Information about the required software versions to implement Smart Licensing Using Policy with SSM On-Prem, is provided below:

Minimum Required SSM On-Prem Version for Smart Licensing Using Policy[3]	Minimum Required Cisco IOS XE Version[4]	Supported Product Instances
Version 8, Release 202102	Cisco IOS XE Amsterdam 17.3.3	• Cisco Catalyst 9800-40 Wireless Controller • Cisco Catalyst 9800-80 Wireless Controller • Cisco Catalyst 9800-L Wireless Controller • Cisco Catalyst 9800-CL Wireless Controller • Cisco Catalyst 9800 embedded Wireless Controller • Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points (EWC-AP)

[3] The minimum required SSM On-Prem version. This means support continues on all subsequent releases - unless noted otherwise

[4] The minimum required software version on the product instance. This means support continues on all subsequent releases - unless noted otherwise.

For more information about SSM On-Prem, see Smart Software Manager On-Prem on the Software Download page. Hover over the .iso image to display the documentation links.

Concepts

This section explains the key concepts of Smart Licensing Using Policy.

License Enforcement Types

A given license belongs to one of three enforcement types. The enforcement type indicates if the license requires authorization before use, or not.

- Unenforced or Not Enforced

  Unenforced licenses *do not* require authorization before use in air-gapped networks, or registration, in connected networks. The terms of use for such licenses are as per the General Terms and Conditions.

  All licenses available on Cisco Catalyst Wireless Controllers are unenforced licenses.

- Enforced

  Licenses that belong to this enforcement type require authorization before use. The required authorization is in the form of an authorization code, which must be installed in the corresponding product instance.

  An example of an enforced license is the Media Redundancy Protocol (MRP) Client license, which is available on Cisco's Industrial Ethernet Switches.

- Export-Controlled

  Licenses that belong to this enforcement type are export-restricted by U.S. trade-control laws and these licenses require authorization before use. The required authorization code must be installed in the corresponding product instance for these licenses as well. Cisco may pre-install export-controlled licenses when ordered with hardware purchase.

  An example of an export-controlled license is the High Speed Encryption (HSECK9) license, which is available on certain Cisco Routers.

License Duration

This refers to the duration or term for which a purchased license is valid. A given license may belong to any one of the enforcement types mentioned above and be valid for the following durations:

- Perpetual: There is no expiration date for such a license.

  AIR Network Essentials and AIR Network Advantage licenses are examples of unenforced, perpetual licenses that are available on Cisco Catalyst Wireless Controllers.

- Subscription: The license is valid only until a certain date.

  AIR Digital Network Architecture (DNA) Essentials and AIR DNA Advantage licenses are examples of unenforced subscription licenses that are available on Cisco Catalyst Wireless Controllers.

Authorization Code

The Smart Licensing Authorization Code (SLAC) allows activation and continued use of a license that is export-controlled or enforced.

A SLAC is not required for any of the licenses available on Cisco Catalyst Wireless Controllers, but if you are upgrading from an earlier licensing model to Smart Licensing Using Policy, you may have a Specific License Reservation (SLR) with its own authorization code. The SLR authorization code is supported after upgrade to Smart Licensing Using Policy.

Note While existing SLRs are carried over after upgrade, you cannot request a new SLR in the Smart Licensing Using Policy environment, because the notion of "reservation" does not apply. For an air-gapped network, the No Connectivity to CSSM and No CSLU topology applies instead

For more information about how the SLR authorization code is handled, see #unique_104. If you want to return an SLR authorization code, see #unique_105.

Policy

A policy provides the product instance with these reporting instructions:

- License usage report acknowledgement requirement (Reporting ACK required): The license usage report is known as a RUM Report and the acknowledgement is referred to as an ACK (See RUM Report and Report Acknowledgement). This is a yes or no value which specifies if the report for this product instance requires CSSM acknowledgement or not. The default policy is always set to "yes".

- First report requirement (days): The first report must be sent within the duration specified here.

  If the value here is zero, no first report is required.

- Reporting frequency (days): The subsequent report must be sent within the duration specified here.

  If the value here is zero, it means no further reporting is required *unless* there is a usage change.

- Report on change (days): In case of a change in license usage, a report must be sent within the duration specified here.

  If the value here is zero, no report is required on usage change.

  If the value here is not zero, reporting *is* required after the change is made. All the scenarios listed below count as changes in license usage on the product instance:

  - Changing licenses consumed (includes changing to a different license, and, adding or removing a license).
  - Going from consuming zero licenses to consuming one or more licenses.
  - Going from consuming one or more licenses to consuming zero licenses.

Note If a product instance has *never* consumed a license, reporting is not required even if the policy has a non-zero value for any of the reporting requirements (First report requirement, Reporting frequency, Report on change).

Understanding Policy Selection

CSSM determines the policy that is applied to a product instance. Only one policy is in use at a given point in time. The policy and its values are based on a number of factors, including the licenses being used.

`Cisco default` is the default policy that is always available in the product instance. If no other policy is applied, the product instance applies this default policy. The table below (#unique_108 unique_108_Connect_42_table_kz1_snm_wmb) shows the `Cisco default` policy values.

While you cannot configure a policy, you can request for a customized one, by contacting the Cisco Global Licensing Operations team. Go to Support Case Manager. Click **OPEN NEW CASE** > Select **Software Licensing**. The licensing team will contact you to start the process or for any additional information. Customized policies are also made available through your Smart account in CSSM.

Note To know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command in privileged EXEC mode.

Table 5: Policy: Cisco default

Policy: `Cisco default`	**Default Policy Values**
Export (Perpetual/Subscription) **Note** Applied only to licenses with enforcement type "Export-Controlled".	Reporting ACK required: Yes First report requirement (days): 0 Reporting frequency (days): 0 Report on change (days): 0

Policy: `Cisco default`	**Default Policy Values**
Enforced (Perpetual/Subscription) **Note** Applied only to licenses with enforcement type "Enforced".	Reporting ACK required: Yes First report requirement (days): 0 Reporting frequency (days): 0 Report on change (days): 0
Unenforced/Non-Export Perpetual[5]	Reporting ACK required: Yes First report requirement (days): 365 Reporting frequency (days): 0 Report on change (days): 90
Unenforced/Non-Export Subscription	Reporting ACK required: Yes First report requirement (days): 90 Reporting frequency (days): 90 Report on change (days): 90

[5] For Unenforced/Non-Export Perpetual: the default policy's first report requirement (within 365 days) applies only if you have purchased hardware or software from a distributor or partner.

RUM Report and Report Acknowledgement

A Resource Utilization Measurement report (RUM report) is a license usage report, which fulfils reporting requirements as specified by the policy. RUM reports are generated by the product instance and consumed by CSSM. The product instance records license usage information and all license usage changes in an open RUM report. At system-determined intervals, open RUM reports are closed and new RUM reports are opened to continue recording license usage. A closed RUM report is ready to be sent to CSSM.

A RUM acknowledgement (RUM ACK or ACK) is a response from CSSM and provides information about the status of a RUM report. Once the ACK for a report is available on the product instance, it indicates that the corresponding RUM report is no longer required and can be deleted.

The reporting method, that is, how a RUM report is sent to CSSM, depends on the topology you implement.

CSSM displays license usage information as per the last received RUM report.

A RUM report may be accompanied by other requests, such as a trust code request, or a SLAC request. So in addition to the RUM report IDs that have been received, an ACK from CSSM may include authorization codes, trust codes, and policy files.

The policy that is applied to a product instance determines the following aspects of the reporting requirement:

- Whether a RUM report is sent to CSSM and the maximum number of days provided to meet this requirement.
- Whether the RUM report requires an acknowledgement (ACK) from CSSM.
- The maximum number of days provided to report a change in license consumption.

If the product instance you are using is a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the conditions for a mandatory ACK starting with Cisco IOS XE Cupertino 17.7.1. For more

information, see RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

RUM report generation, storage, and management

Starting with Cisco IOS XE Cupertino 17.7.1, RUM report generation and related processes have been optimized and enhanced as follows:

- You can display the list of all available RUM reports on a product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). This information is available in the **show license rum**, **show license all**, and **show license tech** privileged EXEC commands. For detailed information about the fields displayed in the output, see the command reference of the corresponding release.
- RUM reports are stored in a new format that reduces processing time, and reduces memory usage. In order to ensure that there are no usage reporting inconsistencies resulting from the difference in the old and new formats, we recommend that you send a RUM report in the method that will apply to your topology, in these situations:

  When you upgrade from an earlier release supporting Smart Licensing Using Policy, to Cisco IOS XE Cupertino 17.7.1 or a later release.

  When you downgrade from Cisco IOS XE Cupertino 17.7.1 or a later release to an earlier release supporting Smart Licensing Using Policy.
- To ensure continued disk space and memory availability, the product instance detects and triggers deletion of RUM reports that are deemed eligible.

Trust Code

A *UDI-tied public key*, which the product instance uses to

- Sign a RUM report. This prevents tampering and ensures data authenticity.
- Enable secure communication with CSSM.

There are multiple ways to obtain a trust code.

- From Cisco IOS XE Cupertino 17.7.1, a trust code is factory-installed for all new orders.

Note A factory-installed trust code cannot be used for *communication* with CSSM.

- A trust code can obtained from CSSM, using an ID token.

  Here you generate an *ID token* in the CSSM Web UI to obtain a trust code and install it on the product instance. You must overwrite the factory-installed trust code if there is one. If a product instance is directly connected to CSSM, use this method to enable the product instance to communicate with CSSM in a secure manner. This method of obtaining a trust code is applicable to all the options of directly connecting to CSSM. For more information, see Connected Directly to CSSM, on page 71.
- From Cisco IOS XE Cupertino 17.7.1, a trust code is automatically obtained in topologies where the product instance initiates the sending of data to CSLU and in topologies where the product instance is in an air-gapped network.

From Cisco IOS XE Cupertino 17.9.1, a trust code is automatically obtained in topologies where CSLU initiates the retrieval of data from the product instance.

If there is a factory-installed trust code, it is automatically overwritten. A trust code obtained this way can be used for secure communication with CSSM.

Refer to the topology description and corresponding workflow to know how the trust code is requested and installed in each scenario: Supported Topologies, on page 69.

If a trust code is installed on the product instance, the output of the **show license status** command displays a timestamp in the `Trust Code Installed:` field.

Supported Topologies

This section describes the various ways in which you can implement Smart Licensing Using Policy. For each topology, refer to the accompanying overview to know the how the set-up is designed to work, and refer to the considerations and recommendations, if any.

After Topology Selection

After you have selected a topology, see #unique_114. These workflows are only for new deployments. They provide the simplest and fastest way to implement a topology.

If you are migrating from an existing licensing model, see #unique_115.

After initial implementation, for any additional configuration tasks you have to perform, for instance, changing the AIR license, or synchronizing RUM reports, see the *Task Library for Smart Licensing Using Policy*.

Note Always check the "Supported topologies" where provided, before you proceed.

Connected to CSSM Through CSLU

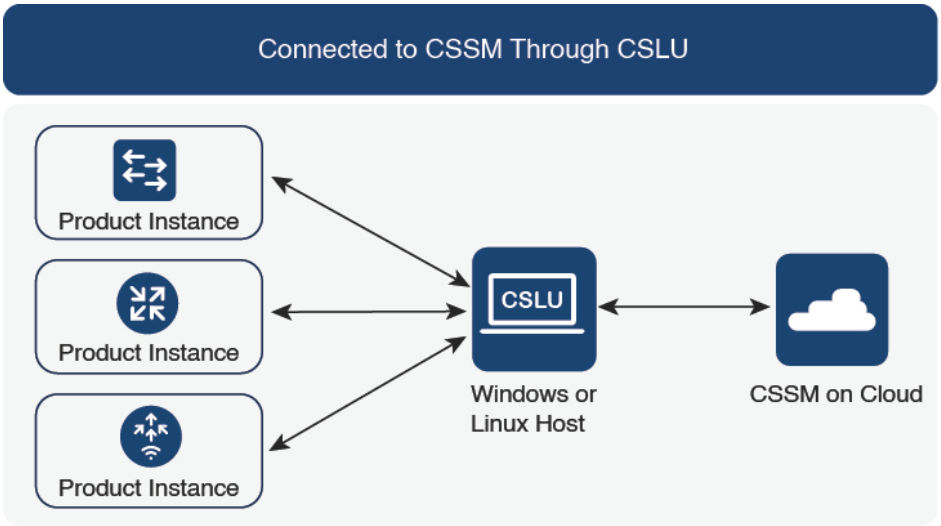
Overview:

Here, product instances in the network are connected to CSLU, and CSLU becomes the single point of interface with CSSM. A product instance can be configured to *push* the required information to CSLU. Alternatively, CSLU can be set-up to *pull* the required information from a product instance at a configurable frequency.

Product instance-initiated communication (push): A product instance initiates communication with CSLU, by connecting to a REST endpoint in CSLU. Data that is sent includes RUM reports and requests for authorization codes, UDI-tied trust codes, and policies. You can configure the product instance to automatically send RUM reports to CSLU at required intervals. This is the default method for a product instance.

CSLU-initiated communication (pull): To initiate the retrieval of information from a product instance, CSLU uses NETCONF, or RESTCONF, or gRPC with YANG models, or native REST APIs, to connect to the product instance. Supported workflows include retrieving RUM reports from the product instance and sending the same to CSSM, authorization code installation, UDI-tied trust code installation, and application of policies.

Figure 2: Topology: Connected to CSSM Through CSLU



Considerations or Recommendations:

Choose the method of communication depending on your network's security policy.

Release-Wise Changes and Enhancements:

This section outlines important release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.7.1:

- Trust code request and installation

  If a trust code is not available on the product instance, the product instance detects and automatically includes a request for one, as part of a RUM report. A corresponding ACK from CSSM includes the trust code. If there is an existing factory-installed trust code, it is automatically overwritten. A trust code obtained this way can be used for communication with CSSM.

  This is supported in a standalone, as well as a High Availability set-up. In a High Availability set-up, the active product instance requests the trust code for all connected product instances where a trust code is not available.

  In this release, this enhancement applies only to the product instance-initiated mode.

From Cisco IOS XE Cupertino 17.9.1:

- Trust code request and installation

  From this release, trust code request and installation is supported in the CSLU-initiated mode as well.

- RUM report throttling

  In the product instance-initiated mode, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down caused by an excessive generation of RUM reports.

You can override the throttling restriction by entering the **license smart sync** command in privileged EXEC mode.

RUM report throttling applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Where to Go Next:

To implement this topology, see #unique_117.

Connected Directly to CSSM

Overview:

This topology is available in the earlier version of Smart Licensing and continues to be supported with Smart Licensing Using Policy.

Here, you establish a *direct* and *trusted* connection from a product instance to CSSM. The direct connection, requires network reachability to CSSM. For the product instance to then exchange messages and communicate with CSSM, configure one of the transport options available with this topology (described below). Lastly, the establishment of trust requires the generation of a token from the corresponding Smart Account and Virtual Account in CSSM, and installation on the product instance.

Note A factory-installed trust code cannot be used for communication with CSSM. This means that for this topology, even if a factory-installed trust code exists, you must obtain a trust code by generating an ID token in CSSM, and you must overwrite the existing factory-installed trust code. Also see: Trust Code, on page 68.

You can configure a product instance to communicate with CSSM in the following ways:

- Use Smart transport to communicate with CSSM

  Smart transport is a transport method where a Smart Licensing (JSON) message is contained within an HTTPs message, and exchanged between a product instance and CSSM, to communicate. The following Smart transport configuration options are available:

  - Smart transport: In this method, a product instance uses a specific Smart transport licensing server URL. This must be configured exactly as shown in the workflow section.
  - Smart transport through an HTTPs proxy: In this method, a product instance uses a proxy server to communicate with the licensing server, and eventually, CSSM.

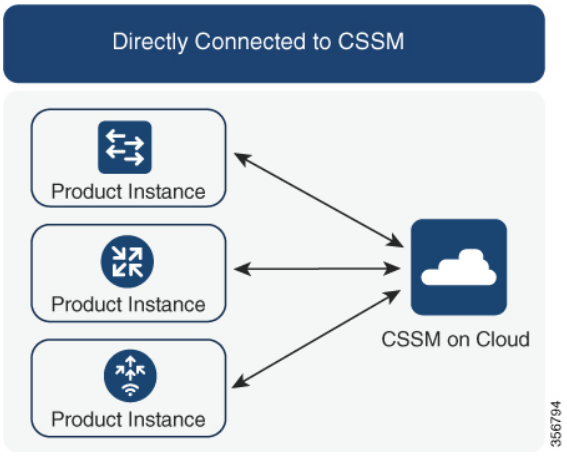
- Use Call Home to communicate with CSSM.

  Call Home provides e-mail-based and web-based notification of critical system events. This method of connecting to CSSM is available in the earlier Smart Licensing environment, and continues to be available with Smart Licensing Using Policy. The following Call Home configuration options are available:

  - Direct cloud access: In this method, a product instance sends usage information directly over the internet to CSSM; no additional components are needed for the connection.

- Direct cloud access through an HTTPs proxy: In this method, a product instance sends usage information over the internet through a proxy server - either a Call Home Transport Gateway or an off-the-shelf proxy (such as Apache) to CSSM.

Figure 3: Topology: Connected Directly to CSSM



Considerations or Recommendations:

Smart transport is the recommended transport method when directly connecting to CSSM. This recommendation applies to:

- New deployments.
- Earlier licensing models. Change configuration after migration to Smart Licensing Using Policy.
- Registered licenses that currently use the Call Home transport method. Change configuration after migration to Smart Licensing Using Policy.
- Evaluation or expired licenses in an earlier licensing model. Change configuration after migration to Smart Licensing Using Policy.

To change configuration after migration, see #unique_118 > Product Instance Configuration > Configure a connection method and transport type > Option 1.

Release-Wise Changes and Enhancements:

This section outlines important release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.9.1:

- RUM report throttling

  The minimum reporting frequency for this topology, is throttled to one day. This means the product instance does not send more than one RUM report a day. This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down caused by an excessive generation of RUM reports.

  You can override the throttling restriction by entering the **license smart sync** command in privileged EXEC mode.

RUM report throttling applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Where to Go Next:

To implement this topology, see #unique_118.

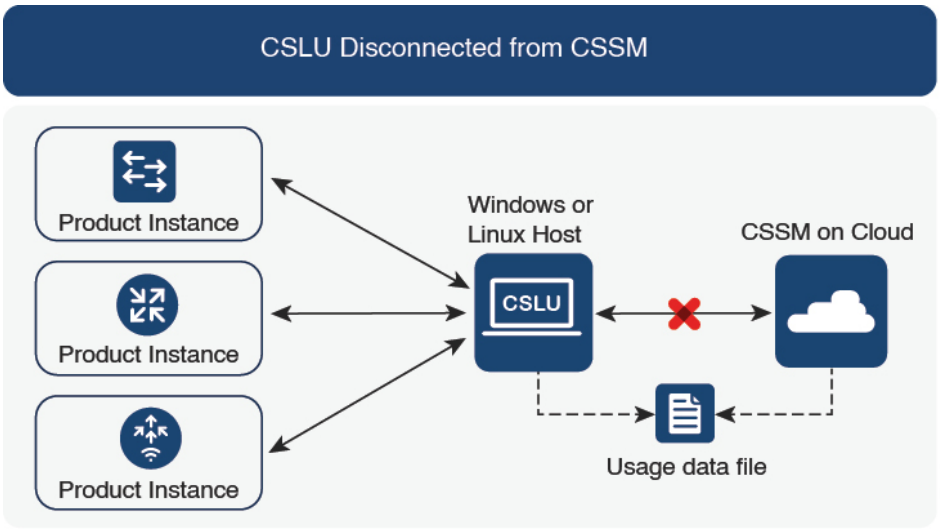
CSLU Disconnected from CSSM

Overview:

Here, a product instance communicates with CSLU, and you have the option of implementing product instance-initiated communication or CSLU-initiated communication (as in the *Connected to CSSM Through CSLU* topology). The other side of the communication, between CSLU and CSSM, is offline. CSLU provides you with the option of working in a mode that is disconnected from CSSM.

Communication between CSLU and CSSM is sent and received in the form of signed files that are saved offline and then uploaded to or downloaded from CSLU or CSSM, as the case may be.

Figure 4: Topology: CSLU Disconnected from CSSM



Considerations or Recommendations:

Choose the method of communication depending on your network's security policy.

Release-Wise Changes and Enhancements:

This section outlines important release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.7.1:

- Trust code request and installation

  If a trust code is not available on the product instance, the product instance detects and automatically includes a request for one, as part of a RUM report that is sent to CSLU, which you upload to CSSM. The ACK that you download from CSSM includes the trust code. If there is an existing factory-installed

trust code, it is automatically overwritten. A trust code obtained this way can be used for communication with CSSM.

This is supported in a standalone, as well as a High Availability set-up. In a High Availability set-up, the active product instance requests the trust code for members or standbys where a trust code is not available.

In this release, this enhancement applies only to the product instance-initiated mode.

From Cisco IOS XE Cupertino 17.9.1:

- Trust code request and installation

  From this release, trust code request and installation is supported in the CSLU-initiated mode as well.

- RUM report throttling

  In the product instance-initiated mode, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down caused by an excessive generation of RUM reports.

  You can override the throttling restriction by entering the **license smart sync** command in privileged EXEC mode.

  RUM report throttling applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Where to Go Next:

To implement this topology, see #unique_120.

Connected to CSSM Through a Controller

When you use a controller to manage a product instance, the controller connects to CSSM, and is the interface for all communication to and from CSSM. The supported controller for Cisco Catalyst Wireless Controllers is Cisco Catalyst Center

Overview:

If a product instance is managed by Cisco Catalyst Center as the controller, the product instance records license usage and saves the same, but it is the Cisco Catalyst Center that initiates communication with the product instance to retrieve RUM reports, report to CSSM, and return the ACK for installation on the product instance.

All product instances that must be managed by Cisco Catalyst Center must be part of its inventory and must be assigned to a site. Cisco Catalyst Center uses the NETCONF protocol to provision configuration and retrieve the required information from the product instance - the product instance must therefore have NETCONF enabled, to facilitate this.

In order to meet reporting requirements, Cisco Catalyst Center retrieves the applicable policy from CSSM and provides the following reporting options:

- Ad hoc reporting: You can trigger an ad hoc report when required.

- Scheduled reporting: Corresponds with the reporting frequency specified in the policy and is automatically handled by Cisco Catalyst Center.

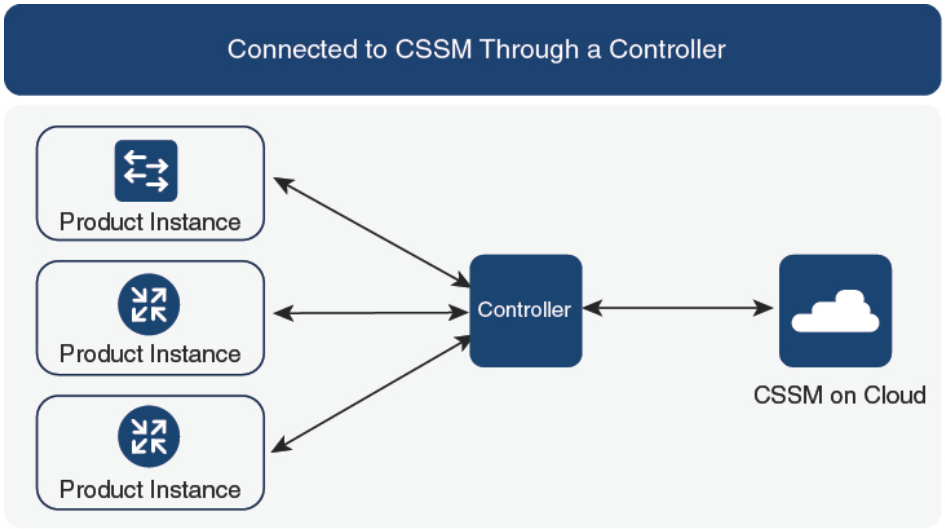
Note Ad hoc reporting must be performed at least once before a product instance is eligible for scheduled reporting.

The first ad hoc report enables Cisco Catalyst Center to determine the Smart Account and Virtual Account to which subsequent RUM reports must be uploaded. You will receive notifications if ad hoc reporting for a product instance has not been performed even once.

Cisco Catalyst Center also enables you to install and remove SLAC for export-controlled licenses. Since all available licenses on Cisco Catalyst Wireless Controllers are unenforced licenses, SLAC installation and removal do not apply.

A trust code is *not* required.

Figure 5: Topology: Connected to CSSM Through a Controller



Considerations or Recommendations:

This is the recommended topology if you are using Cisco Catalyst Center.

Where to Go Next:

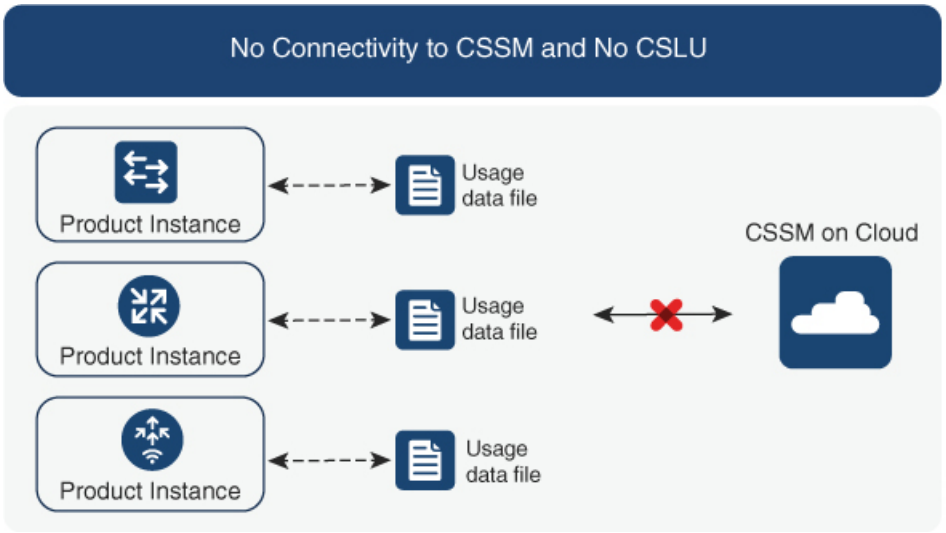
To implement this topology, see Workflow for Topology: Connected to CSSM Through a Controller, on page 93.

No Connectivity to CSSM and No CSLU

Overview:

Here you have a product instance and CSSM disconnected from each other, and without any other intermediary utilities or components. All communication is in the form of uploaded and downloaded files. These files can be RUM reports and requests for UDI-tied trust codes.

Figure 6: Topology: No Connectivity to CSSM and No CSLU



Considerations or Recommendations:

This topology is suited to a high-security deployment where a product instance cannot communicate online, with anything outside its network.

Release-Wise Changes and Enhancements

This section outlines the release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.7.1:

- Trust code request and installation

  If a trust code is not available on the product instance, the product instance automatically includes a trust code request in the RUM report that you save, to upload to CSSM. The ACK that you then download from CSSM includes the trust code.

  If there is a factory-installed trust code, it is automatically overwritten when you install the ACK. A trust code obtained this way can be used for secure communication with CSSM.

  This is supported in a standalone, as well as a High Availability set-up. In a High Availability set-up, the active product instance requests the trust code for all connected product instances where a trust code is not available.

- Simpler authorization code return

  A simpler way to upload an authorization code return file is available in the CSSM Web UI. You do not have to locate the product instance in the correct Virtual Account in the CSSM Web UI any longer. You can upload the return file, as you would a RUM report.

Where to Go Next:

To implement this topology, see #unique_124.

SSM On-Prem Deployment

Overview:

SSM On-Prem is designed to work as an extension of CSSM that is deployed on your premises.

Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. Each instance of SSM On-Prem must be made known to CSSM through a mandatory registration and synchronization of the local account in SSM On-Prem, with a Virtual Account in CSSM.

When you deploy SSM On-Prem to manage a product instance, the product instance can be configured to *push* the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* the required information from a product instance at a configurable frequency.

- Product instance-initiated communication (push): The product instance initiates communication with SSM On-Prem, by connecting to a REST endpoint in SSM On-Prem. Data that is sent includes RUM reports and requests for authorization codes, trust codes, and policies.

  Options for communication between the product instance and SSM On-Prem in this mode:

  - Use a CLI command to push information to SSM On-Prem as and when required.
  - Use a CLI command and configure a reporting interval, to automatically send RUM reports to SSM On-Prem at a scheduled frequency.

- SSM On-Prem-initiated communication (pull): To initiate the retrieval of information from a product instance, SSM On-Prem NETCONF, RESTCONF, and native REST API options, to connect to the product instance. Supported workflows include receiving RUM reports from the product instance and sending the same to CSSM, authorization code installation, trust code installation, and application of policies.

  Options for communication between the product instance and SSM On-Prem in this mode:

  - Collect usage information from one or more product instances as and when required (on-demand).
  - Collect usage information from one or more product instances at a scheduled frequency.

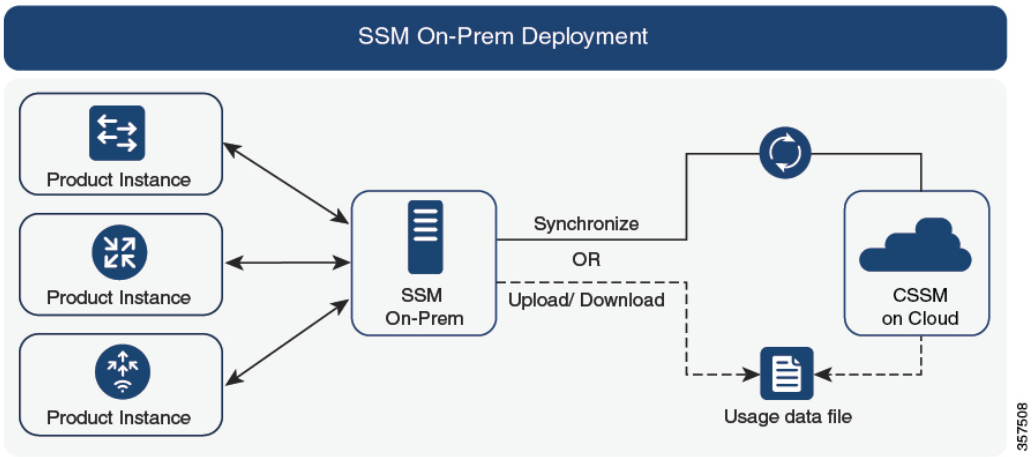
In SSM On-Prem, the reporting interval is set to the default policy on the product instance. You can change this, but only to report more frequently (a narrower interval), or you can install a custom policy if available.

After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Options for usage synchronization between SSM On-Prem and CSSM – for the push *and* pull mode:

- Perform ad-hoc synchronization with CSSM (Synchronize now with Cisco).
- Schedule synchronization with CSSM for specified times.
- Communicate with CSSM through signed files that are saved offline and then upload to or download from SSM On-Prem or CSSM, as the case may be.

Note This topology involves two different kinds of synchronization between SSM On-Prem and CSSM. The first is where the *local account* is synchronized with CSSM - this is for the SSM On-Prem instance to be known to CSSM and is performed by using the **Synchronization** widget in SSM On-Prem. The second is where *license usage* is synchronized with CSSM, either by being connected to CSSM or by downloading and uploading files. You must synchronize the local account before you can synchronize license usage.

Figure 7: Topology: SSM On-Prem Deployment



Considerations or Recommendations:

This topology is suited to the following situations:

- If you want to manage your product instances on your premises, as opposed communicating directly with CSSM for this purpose.
- If your company's policies prevent your product instances from reporting license usage directly to Cisco (CSSM).
- If your product instances are in an air-gapped network and cannot communicate online, with anything outside their network.

Apart from support for Smart Licensing Using Policy, some of the key benefits of SSM On-Prem *Version 8* include:

- Multi-tenancy: One tenant constitutes one Smart Account-Virtual Account pair. SSM On-Prem enables you to manage multiple pairs. Here you create local accounts that reside in SSM On-Prem. Multiple local accounts roll-up to a Smart Account-Virtual Account pair in CSSM. For more information, see the Cisco Smart Software Manager On-Prem User Guide > *About Accounts and Local Virtual Accounts*.

Note The relationship between CSSM and SSM On-Prem instances is still one-to-one.

- Scale: Supports up to a total of 300,000 product instances

- High-Availability: Enables you to run two SSM On-Prem servers in the form of an active-standby cluster. For more information, see the Cisco Smart Software On-Prem Installation Guide > Appendix 4. Managing a High Availability (HA) Cluster in Your System.

  High-Availability deployment is supported on the SSM On-Prem console and the required command details are available in the Cisco Smart Software On-Prem Console Guide.

- Options for online and offline connectivity to CSSM.

SSM On-Prem Limitations:

- Proxy support for communication with CSSM, for the purpose of *license usage* synchronization is available only from Version 8 202108 onwards. The use of a proxy for *local account* synchronization, which is performed by using the **Synchronization** widget, is available from the introductory SSM On-Prem release where Smart Licensing Using Policy is supported.
- SSM On-Prem-initiated communication is not supported on a product instance that is in a Network Address Translation (NAT) set-up. You must use product instance-initiated communication, and further, you must *enable* SSM On-Prem to support a product instance that is in a NAT setup. Details are provided in the workflow for this topology.

Release-Wise Changes and Enhancements:

This section outlines important release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.9.1:

- RUM report throttling

  In the product instance-initiated mode, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down caused by an excessive generation of RUM reports.

  You can override the throttling restriction by entering the **license smart sync** command in privileged EXEC mode.

  RUM report throttling applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Where to Go Next:

To implement this topology, see Workflow for Topology: SSM On-Prem Deployment, on page 95

If you are migrating from an existing version of SSM On-Prem, the sequence in which you perform the various upgrade-related activities is crucial. See Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 119

Interactions with Other Features

High Availability

This section explains considerations that apply to a High Availability configuration, when running a software version that supports Smart Licensing Using Policy. The following High Availability set-ups are within the scope of this document:

A dual-chassis set-up (could be fixed or modular), with the active in one chassis and a standby in the other chassis.

A wireless N+1 topology, where "n" number of wireless controllers act as primary and a "+1" wireless controller acts as the secondary or fallback wireless controller for Access Points (APs). Each Access Point is configured with a primary and a secondary wireless controller. In case of a failure on the primary, all access points that were connected to the primary now fallback to the secondary wireless controller.

Trust Code Requirements in a High Availability Set-Up

The number of trust codes required depends on the number of UDIs. The active product instance can submit requests for all devices in the High Availability set-up and install all the trust codes that are returned in an ACK.

Policy Requirements in a High Availability Set-Up

There are no policy requirements that apply exclusively to a High Availability set-up. As in the case of a standalone product instance, only one policy exists in a High Availability set-up as well, and this is on the active. The policy on the active applies to any standbys in the set-up.

Product Instance *Functions* in a High Availability Set-Up

This section explains general product instance functions in a High Availability set-up, as well as what the product instance does when a new standby or secondary is added to an existing High Available set-up.

For authorization and trust codes: The active product instance can request (if required) and install authorization codes and trust codes for standbys.

For policies: The active product instance synchronizes with the standby.

For reporting: Only the active product instance reports usage. The active reports usage information for all devices in the High Availability set-up. In addition to scheduled reporting, the following events trigger reporting:

- The addition or removal of a standby. The RUM report includes information about the standby that was added or removed.
- A switchover.
- A reload.

When one of the above events occur, the "Next report push" date of the **show license status** privileged EXEC command is updated. But it is the implemented topology and associated reporting method that determine if the report is sent by the product instance or not. For example, if you have implemented a topology where the product instance is disconnected (Transport Type is Off), then the product instance does not send RUM reports even if the "Next report push" date is updated.

For addition or removal of a new standby:

- A product instance that is connected to CSLU, does not take any further action.
- A product instance that is directly connected to CSSM, performs trust synchronization. Trust synchronization involves the following:

  Installation of trust code on the standby if not installed already.

  If a trust code is already installed, the trust synchronization process ensures that the new standby is in the same Smart Account and Virtual Account as the active. If it is not, the new standby is *moved* to the same Smart Account and Virtual Account as the active.

  Installation of an authorization code, policy, and purchase information, if applicable

  Sending of a RUM report with current usage information.

For addition or removal of a secondary:

There are no product instance functions that apply exclusively to the addition or removal of a secondary product instance. Further, all the secondary product instances are in the same Smart Account and Virtual Account as the primary product instance.

Upgrades

This section explains the following aspects:

Migrating from earlier licensing models to Smart Licensing Using Policy. When migrating from earlier licensing models, also see the #unique_115 section for examples of migration scenarios that apply to Cisco Catalyst Wireless Controllers.

Upgrading in the Smart Licensing Using Policy environment - where the software version you are upgrading from and the software version you are upgrading to, both support Smart Licensing Using Policy.

Identifying the Current Licensing Model Before Upgrade

Before you upgrade to Smart Licensing Using Policy, if you want to know the current licensing model that is effective on the product instance, enter the **show license all** command in privileged EXEC mode.

How Upgrade Affects Enforcement Types for Existing Licenses

When you upgrade to a software version which supports Smart Licensing Using Policy, the way existing licenses are handled, depends primarily on the license enforcement type.

- An unenforced license that was being used before upgrade, continues to be available after the upgrade. All licenses on Cisco Catalyst Wireless Controllers are unenforced licenses. This includes licenses from all earlier licensing models:
  - Smart Licensing
  - Specific License Reservation (SLR), which has an accompanying authorization code. The authorization code continues to be valid after upgrade to Smart Licensing Using Policy and authorizes existing license consumption.
  - Evaluation or expired licenses from any of the above mentioned licensing models.
- An enforced or export-controlled license that was being used before upgrade, continues to be available after upgrade if the required authorization exists.

There are no export-controlled or enforced licenses on any of the supported Cisco Catalyst Wireless Controllers, therefore, these enforcement types and the requisite SLAC do not apply.

How Upgrade Affects Reporting for Existing Licenses

Existing License	Reporting Requirements After Migration to Smart Licensing Using Policy
Specific License Reservation (SLR)	Required only if there is a change in license consumption. An existing SLR authorization code authorizes existing license consumption after upgrade to Smart Licensing Using Policy.
Smart Licensing (Registered and Authorized license)	Depends on the policy.
Evaluation or expired licenses	Based on the reporting requirements of the Cisco default policy.

How Upgrade Affects Transport Type for Existing Licenses

The transport type, if configured in your existing set-up, is retained after upgrade to Smart Licensing Using Policy.

When compared to the earlier version of Smart Licensing, additional transport types are available with Smart Licensing Using Policy. There is also a change in the default transport mode. The following table clarifies how this may affect upgrades:

Transport type Before Upgrade	License or License State Before Upgrade	Transport Type After Upgrade
Default (callhome)	evaluation	cslu (default in Smart Licensing Using Policy)
	SLR	off
	registered	callhome
smart	evaluation	off
	SLR	off
	registered	smart

How Upgrade Affects the Token Registration Process

In the earlier version of Smart Licensing, a token was used to register and connect to CSSM. ID token registration is not required in Smart Licensing Using Policy. The token generation feature is still available in CSSM, and is used to *establish trust* when a product instance is directly connected to CSSM. See Connected Directly to CSSM.

Upgrades Within the Smart Licensing Using Policy Environment

This section covers any release-specific considerations or actions that apply when you upgrade the product instance from one release where Smart Licensing Using Policy is supported to another release where Smart Licensing Using Policy is supported.

Starting with Cisco IOS XE Cupertino 17.7.1, RUM reports are stored in a format that reduces processing time. In order to ensure that there are no usage reporting inconsistencies resulting from the differences in the old and new formats, we recommend completing one round of usage reporting as a standard practice when upgrading from an earlier release that supports Smart Licensing Using Policy, to Cisco IOS XE Cupertino 17.7.1 or a later release.

Downgrades

This section provides information about downgrades to an earlier licensing model, for new deployments and existing deployments. It also covers information relevant to downgrades within in the Smart Licensing Using Policy environment.

New Deployment Downgrade

This section describes considerations and actions that apply if a newly purchased product instance with a software version where Smart Licensing Using Policy is enabled by default, is downgraded to a software version where Smart Licensing Using Policy is not supported.

The outcome of the downgrade depends on whether a trust code was installed while still operating in the Smart Licensing Using Policy environment, and further action may be required depending on the release you downgrade to.

If the topology you implemented while in the Smart Licensing Using Policy environment was "Connected Directly to CSSM", then a trust code installation can be expected or assumed, because it is required as part of topology implementation. For any of the other topologies, trust establishment is not mandatory. Downgrading product instances with one of these other topologies will therefore mean that you have to restore licenses to a registered and authorized state by following the procedures that are applicable in the Smart Licensing environment. See the table (*Outcome and Action for New Deployment Downgrade to Smart Licensing*) below.

Table 6: Outcome and Action for New Deployment Downgrade to Smart Licensing

In the Smart Licensing Using Policy Environment	Downgrade to..	Outcome and Further Action
Standalone product instance, connected directly to CSSM, and trust established.	Cisco IOS XE Amsterdam 17.3.1 OR Cisco IOS XE Gibraltar 16.12.4 and later releases in Cisco IOS XE Gibraltar 16.12.x	No further action is required. The product instance attempts to renew trust with CSSM after downgrade. After a successful renewal, licenses are in a registered state and the earlier version of Smart Licensing is effective on the product instance.
	Any other release (other than the ones mentioned in the row above) that supports Smart Licensing	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, configure the **license smart register idtoken** *idtoken* command in global configuration mode.
High Availability set-up, connected directly to CSSM, and trust established.	Any release that supports Smart Licensing	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, configure the **license smart register idtoken** *idtoken* **all** command in global configuration mode.
Any other topology. (Connected to CSSM Through CSLU, CSLU Disconnected from CSSM, No Connectivity to CSSM and No CSLU)	Any release that supports Smart Licensing	Action is required. Restore licenses to a registered and authorized state by following the procedures that are applicable in the Smart Licensing environment.

Upgrade and Then Downgrade

This section describes considerations and actions that apply if a product instance is upgraded to a software version that supports Smart Licensing Using Policy and then downgraded to an earlier licensing model.

When you downgrade such a product instance, *license consumption does not change* and any product features you have configured on the product instance are preserved – only the features and functions that are available with Smart Licensing Using Policy are not available anymore. Refer to the corresponding section below to know more about reverting to an earlier licensing model.

Upgrade to Smart Licensing Using Policy and then Downgrade to Smart Licensing

The outcome of the downgrade depends on whether a trust code was installed while you were still operating in the Smart Licensing Using Policy environment, and further action may be required depending on the release you downgrade to. See the table below.

Table 7: Outcome and Action for Upgrade to Smart Licensing Using Policy and then Downgrade to Smart Licensing

In the Smart Licensing Using Policy Environment	Downgrade to..	Outcome and Further Action
Standalone product instance, connected directly to CSSM, and trust established.	Cisco IOS XE Amsterdam 17.3.1 OR Cisco IOS XE Gibraltar 16.12.4 and later releases in Cisco IOS XE Gibraltar 16.12.x	No further action is required. The system recognizes the trust code and converts it back to a registered ID token, and this reverts the license to an AUTHORIZED and REGISTERED state.
	Any other release (other than the ones mentioned in the row above) that supports Smart Licensing	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, configure the **license smart register idtoken***idtoken* command in global configuration mode.
High Availability set-up, connected directly to CSSM, and trust established.	Any release that supports Smart Licensing	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, configure the **license smart register idtoken** *idtoken* **all** command in global configuration mode.
Any other topology (Connected to CSSM Through CSLU, CSLU Disconnected from CSSM, No Connectivity to CSSM and No CSLU)	Any release that supports Smart Licensing.	Action is required. Restore licenses to a registered and authorized state by following the procedures that are applicable in the Smart Licensing environment.

Note Licenses that were in an evaluation or expired state in the Smart Licensing environment, revert to that same state after downgrade.

Upgrade to Smart Licensing Using Policy and then Downgrade to SLR

To revert to SLR, all that is required is for the image to be downgraded. The license remains reserved and authorized – no further action is required.

However, if you have returned an SLR while in the Smart Licensing Using Policy environment, then you must repeat the process of procuring an SLR as required, in the supported release.

Downgrades Within the Smart Licensing Using Policy Environment

This section covers any release-specific considerations or actions that apply when you downgrade the product instance from one release where Smart Licensing Using Policy is supported to another release where Smart Licensing Using Policy is supported.

Starting with Cisco IOS XE Cupertino 17.7.1, RUM reports are stored in a format that reduces processing time. In order to ensure that there are no usage reporting inconsistencies resulting from the differences in the old and new formats, we recommend completing one round of usage reporting as a standard practice when downgrading from Cisco IOS XE Cupertino 17.7.1 or a later release to an earlier release supporting Smart Licensing Using Policy.

How to Configure Smart Licensing Using Policy: Workflows by Topology

This section provides the simplest and fastest way to implement a topology.

Note These workflows are meant for new deployments only. If you are migrating from an existing licensing model, see #unique_115.

Workflow for Topology: Connected to CSSM Through CSLU

Depending on whether you want to implement a product instance-initiated or CSLU-initiated method of communication, complete the corresponding sequence of tasks:

- Tasks for Product Instance-Initiated Communication
- Tasks for CSLU-Initiated Communication

Tasks for Product Instance-Initiated Communication

CSLU Installation → CSLU Preference Settings → Product Instance Configuration

1. ***CSLU Installation***

   Where task is performed: A laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

   Download the file from Smart Software Manager > **Smart Licensing Utility**.

   Refer to Cisco Smart License Utility Quick Start Setup Guide and Cisco Smart Licensing Utility User Guide for help with installation and set-up.

2. ***CSLU Preference Settings***

   Where tasks are performed: CSLU

   a. #unique_144

b. #unique_145

c. #unique_146

3. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

   a. #unique_147

   b. Ensure that transport type is set to **cslu**.

   CSLU is the default transport type. If you have configured a different option, enter the **license smart transport cslu** command in global configuration mode. Save any changes to the configuration file.

   ```
   Device(config)# license smart transport cslu
   Device(config)# exit
   Device# copy running-config startup-config
   ```

   c. Specify how you want CSLU to be discovered (*choose one*):

   - Option 1:

     No action required. Name server configured for Zero-touch DNS discovery of `cslu-local`

     Here, if you have configured DNS (the name server IP address is configured on the product instance), and the DNS server has an entry where hostname `cslu-local` is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname `cslu-local`.

   - Option 2:

     No action required. Name server and domain configured for Zero-touch DNS discovery of `cslu-local.<domain>`

     Here if you have configured DNS (the name server IP address and domain is configured on the product instance), and the DNS server has an entry where `cslu-local.<domain>` is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname `cslu-local`.

   - Option 3:

     Configure a specific URL for CSLU.

     Enter the **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* command in global configuration mode. For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

     ```
     Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi
     Device(config)# exit
     Device# copy running-config startup-config
     ```

Result:

Since the product instance initiates communication, it automatically sends out the first RUM report at the scheduled time, as per the policy. Along with this first report, if applicable, it sends a request for a UDI-tied trust code. CSLU forwards the RUM report to CSSM and retrieves the ACK, which also contains the trust code. The ACK is applied to the product instance the next time the product instance contacts CSLU.

In the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and all subsequent releases from Cisco IOS XE Cupertino 17.9.1 onwards: The product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and CSSM, by entering the **license smart sync** command in privileged EXEC mode.

To know when the product instance will be sending the next RUM report, enter the **show license all** command in privileged EXEC mode and in the output, check the date in the `Next report push` field.

To verify trust code installation, enter the **show license status** command in privileged EXEC mode. Check for the updated timestamp in the `Trust Code Installed` field.

In case of a change in license usage, see #unique_148 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Tasks for CSLU-Initiated Communication

CSLU Installation → CSLU Preference Settings→ Product Instance Configuration → Usage Synchronization

1. ***CSLU Installation***

   Where task is performed: A laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

   Download the file from Smart Software Manager > **Smart Licensing Utility**.

   Refer to Cisco Smart License Utility Quick Start Setup Guide and Cisco Smart Licensing Utility User Guide for help with installation and set-up.

2. ***CSLU Preference Settings***

   Where tasks is performed: CSLU

   a. #unique_144

   b. #unique_145

   c. #unique_149

3. ***Product Instance Configuration***

   Where tasks is performed: Product Instance

   #unique_150

4. ***Usage Synchronization***

   Where tasks is performed: Product Instance

   #unique_151

Result:

Since CSLU is logged into CSSM, the reports are automatically sent to the associated Smart Account and Virtual Account in CSSM and CSSM will send an ACK to CSLU as well as to the product instance. It gets the ACK from CSSM and sends this back to the product instance for installation. The ACK from CSSM contains the trust code and SLAC if this was requested.

In case of a change in license usage, see #unique_148 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Trust code request and installation is supported starting with Cisco IOS XE Cupertino 17.9.1.

Workflow for Topology: Connected Directly to CSSM

Smart Account Set-Up → Product Instance Configuration → Trust Establishment with CSSM

1. ***Smart Account Set-Up***

   Where task is performed: CSSM Web UI, https://software.cisco.com/

   Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

2. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

   a. Set-Up product instance connection to CSSM: #unique_153

   b. Configure a connection method and transport type (choose one)

   - Option 1:

     Smart transport: Set transport type to **smart** and configure the corresponding URL.

     If the transport mode is set to **license smart transport smart**, and you configure **license smart url default**, the Smart URL (https://smartreceiver.cisco.com/licservice/license) is automatically configured. Save any changes to the configuration file.

     ```
     Device(config)# license smart transport smart
     Device(config)# license smart url default
     Device(config)# exit
     Device# copy running-config startup-config
     ```

   - Option 2:

     Configure Smart transport through an HTTPs proxy. See #unique_154

   - Option 3:

     Configure Call Home service for direct cloud access. See #unique_155.

   - Option 4:

     Configure Call Home service for direct cloud access through an HTTPs proxy. See #unique_156.

3. ***Trust Establishment with CSSM***

   Where task is performed: CSSM Web UI and then the product instance

   a. Generate one token for each *Virtual Account* you have. You can use same token for all the product instances that are part of one Virtual Account: #unique_157

   b. Having downloaded the token, you can now install the trust code on the product instance: #unique_158

Result:

After establishing trust, CSSM returns a policy. The policy is automatically installed on all product instances of that Virtual Account. The policy specifies if and how often the product instance reports usage.

In the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and all subsequent releases from Cisco IOS XE Cupertino 17.9.1 onwards: The product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and CSSM, by entering the **license smart sync** command in privileged EXEC mode.

To change the reporting interval, configure the **license smart usage interval** command in global configuration mode. For syntax details see the *license smart (privileged EXEC)* command in the Command Reference for the corresponding release.

In case of a change in license usage, see #unique_148 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Workflow for Topology: CSLU Disconnected from CSSM

Depending on whether you want to implement a product instance-initiated or CSLU-initiated method of communication. Complete the corresponding table of tasks below.

- Tasks for Product Instance-Initiated Communication
- Tasks for CSLU-Initiated Communication

Tasks for Product Instance-Initiated Communication

CSLU Installation → CSLU Preference Settings → Product Instance Configuration→ Usage Synchronization

1. ***CSLU Installation***

   Where task is performed: A laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

   Download the file from Smart Software Manager > **Smart Licensing Utility**.

   Refer to Cisco Smart License Utility Quick Start Setup Guide and Cisco Smart Licensing Utility User Guide for help with installation and set-up.

2. ***CSLU Preference Settings***

   Where tasks are performed: CSLU

   a. In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to **off**. The field switches to “Cisco Is Not Available”.

   b. #unique_145

   c. #unique_146

3. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

a. #unique_147

b. Ensure that transport type is set to **cslu**.

CSLU is the default transport type. If you have configured a different option, enter the **license smart transport cslu** command in global configuration mode. Save any changes to the configuration file.

```
Device(config)# license smart transport cslu
Device(config)# exit
Device# copy running-config startup-config
```

c. Specify how you want CSLU to be discovered (*choose one*)

- Option 1:

  No action required. Name server configured for Zero-touch DNS discovery of `cslu-local`

  Here, if you have configured DNS (the name server IP address is configured on the product instance), and the DNS server has an entry where hostname `cslu-local` is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname `cslu-local`.

- Option 2:

  No action required. Name server and domain configured for Zero-touch DNS discovery of `cslu-local.<domain>`

  Here if you have configured DNS (the name server IP address and domain is configured on the product instance), and the DNS server has an entry where `cslu-local.<domain>` is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname `cslu-local`.

- Option 3:

  Configure a specific URL for CSLU.

  Enter the **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* command in global configuration mode. For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

  ```
  Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi
  Device(config)# exit
  Device# copy running-config startup-config
  ```

4. ***Usage Synchronization***

Where tasks are performed: CSLU and CSSM

Since the product instance initiates communication, it automatically sends out the first RUM report at the scheduled time, as per the policy. You can also enter the **license smart sync** privileged EXEC command to trigger this. Along with this first report, if applicable, it sends a request for a UDI-tied trust code. Since CSLU is disconnected from CSSM, perform the following tasks to send the RUM Reports to CSSM.

a. #unique_160

b. #unique_161

c. #unique_162

Result:

The ACK you have imported from CSSM contains the trust code if this was requested. The ACK is applied to the product instance the next time the product instance contacts CSLU.

In the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and all subsequent releases from Cisco IOS XE Cupertino 17.9.1 onwards: The product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and CSSM, by entering the **license smart sync** command in privileged EXEC mode.

To know when the product instance will be sending the next RUM report, enter the **show license all** command in privileged EXEC mode and in the output, check the date for the `Next report push` field.

To verify trust code installation, enter the `show license status` command in privileged EXEC mode. Check for the updated timestamp in the `Trust Code Installed` field.

In case of a change in license usage, see #unique_148 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Tasks for CSLU-Initiated Communication

CSLU Installation → CSLU Preference Settings → Product Instance Configuration → Usage Synchronization

1. ***CSLU Installation***

   Where task is performed: A laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

   Download the file from Smart Software Manager > **Smart Licensing Utility**.

   Refer to Cisco Smart License Utility Quick Start Setup Guide and Cisco Smart Licensing Utility User Guide for help with installation and set-up.

2. ***CSLU Preference Settings***

   Where tasks is performed: CSLU

   a. In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to **off**. The field switches to “Cisco Is Not Available”.

   b. #unique_145

   c. #unique_149

   d. #unique_151

3. ***Product Instance Configuration***

   Where task is performed: Product Instance

   #unique_150

4. ***Usage Synchronization***

   Where tasks are performed: CSLU and CSSM

Collect usage data from the product instance. Since CSLU is disconnected from CSSM, you then save usage data which CSLU has collected from the product instance to a file. Along with this first report, if applicable, an authorization code and a UDI-tied trust code request is included in the RUM report. Then, from a workstation that is connected to Cisco, upload it to CSSM. After this, download the ACK from CSSM. In the workstation where CSLU is installed and connected to the product instance, upload the file to CSLU.

a. #unique_160

b. #unique_161

c. #unique_162

Result:

The ACK you have imported from CSSM contains the trust code and SLAC if this was requested. The uploaded ACK is applied to the product instance the next time CSLU runs an update.

In case of a change in license usage, see #unique_148 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Trust code request and installation is supported starting with Cisco IOS XE Cupertino 17.9.1.

Workflow for Topology: Connected to CSSM Through a Controller

To deploy Cisco Catalyst Center as the controller, complete the following workflow:

Product Instance Configuration → Cisco Catalyst Center **Configuration**

1. ***Product Instance Configuration***

   Where task is performed: Product Instance

   Enable NETCONF. Cisco Catalyst Center uses the NETCONF protocol to provision configuration and retrieve the required information from the product instance - the product instance must therefore have NETCONF enabled, to facilitate this.

   For more information, see the Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.3.x. In the guide, go to *Model-Driven Programmability* > *NETCONF Protocol*.

2. ***Cisco Catalyst Center Configuration***

   Where tasks is performed: Cisco Catalyst Center GUI

   An outline of the tasks you must complete and the accompanying documentation reference is provided below. The document provides detailed steps you have to complete in the Cisco Catalyst Center GUI:

   a. Set-up the Smart Account and Virtual Account.

   Enter the same log in credentials that you use to log in to the CSSM Web UI. This enables Cisco Catalyst Center to establish a connection with CSSM.

   See the *Cisco Catalyst Center Administrator Guide* of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Set Up License Manager*.

   b. Add the required product instances to Cisco Catalyst Center inventory and assign them to a site.

This enables Cisco Catalyst Center to push any necessary configuration, including the required certificates, for Smart Licensing Using Policy to work as expected.

See the *Cisco Catalyst Center User Guide* of the required release (Release 2.2.2 onwards) > *Display Your Network Topology* > *Assign Devices to a Site*.

Result:

After you implement the topology, *you* must trigger the very first ad hoc report in Cisco Catalyst Center, to establish a mapping between the Smart Account and Virtual Account, and product instance. See the *Cisco Catalyst Center Administrator Guide* of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Upload Resource Utilization Details to CSSM*. Once this is done, Cisco Catalyst Center handles subsequent reporting based on the reporting policy.

If multiple policies are available, Cisco Catalyst Center maintains the narrowest reporting interval. You can change this, but only to report more frequently (a narrower interval). See the *Cisco Catalyst Center Administrator Guide* of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Modify License Policy*.

If you want to change the license level after this, see the *Cisco Catalyst Center Administrator Guide* of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Change License Level*.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Workflow for Topology: No Connectivity to CSSM and No CSLU

Since you do not have to configure connectivity to any other component, the list of tasks required to set-up the topology is a small one. See, the ***Results*** section at the end of the workflow to know how you can complete requisite usage reporting after you have implemented this topology.

Product Instance Configuration

Where task is performed: Product Instance

Set transport type to **off**.

Enter the **license smart transport off** command in global configuration mode. Save any changes to the configuration file.

```
Device(config)# license smart transport off
Device(config)# exit
Device# copy running-config startup-config
```

Result:

All communication to and from the product instance is disabled. To report license usage you must save RUM reports to a file on the product instance. From a workstation that has connectivity to the Internet and Cisco, upload the file to CSSM:

1. Generate and save RUM reports

   Enter the **license smart save usage** command in privileged EXEC mode. In the example below, all RUM reports are saved to the flash memory of the product instance, in file `all_rum.txt`.

Starting with Cisco IOS XE Cupertino 17.7.1, if a trust code does not already exist on the product instance, configuring this command automatically includes a trust code request in the RUM report. This is supported in a standalone, as well as a High Availability set-up.

In the example below, the file is first saved to bootflash and then copied to a TFTP location:

```
Device# license smart save usage all file bootflash:all_rum.txt
Device# copy bootflash:all_rum.txt tftp://10.8.0.6/all_rum.txt
```

2. Upload usage data to CSSM: #unique_161.
3. Install the ACK on the product instance: #unique_164

If you want to change license usage, see #unique_148.

If you want to return an SLR authorization code, see Removing and Returning an Authorization Code, on page 151.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Workflow for Topology: SSM On-Prem Deployment

Depending on whether you want to implement a product instance-initiated (push) or SSM On-Prem-initiated (pull) method of communication, complete the corresponding sequence of tasks.

Tasks for Product Instance-Initiated Communication

SSM On-Prem Installation → Addition and Validation of Product Instances (Only if Applicable) → Product Instance Configuration→ Initial Usage Synchronization

1. ***SSM On-Prem Installation***

   Where task is performed: A physical server such as a Cisco UCS C220 M3 Rack Server, or a hardware-based server that meets the necessary requirements.

   Download the file from Smart Software Manager > **Smart Software Manager On-Prem**.

   Refer to the *Cisco Smart Software On-Prem Installation Guide* and the *Cisco Smart Software On-Prem User Guide* for help with installation.

   Installation is complete when you have deployed SSM On-Prem, configured a common name on SSM On-Prem (**Security Widget** > **Certificates**), synchronized the NTP server (**Settings** widget > **Time Settings**), and created, registered, and synchronized (**Synchronization** widget) the SSM On-Prem local account with your Smart Account and Virtual Account in CSSM.

Note Licensing functions in the **On-Prem Licensing Workspace** are greyed-out until you complete the creation, registration, and synchronization of the local account with your Smart Account in CSSM. The *local account*synchronization with CSSM is for the SSM On-Prem instance to be known to CSSM, and is different from usage synchronization which is performed in **4. Initial Usage Synchronization** below.

2. ***Addition and Validation of Product Instances***

   Where tasks are performed: SSM On-Prem UI

This step ensures that the product instances are validated and mapped to the applicable Smart Account and Virtual account in CSSM. This step is required only in the following cases:

- If you want your product instances to be added and validated in SSM On-Prem before they are reported in CSSM (for added security).
- If you have created local virtual accounts (in addition to the default local virtual account) in SSM On-Prem. In this case you must provide SSM On-Prem with the Smart Account and Virtual Account information for the product instances in these local virtual accounts, so that SSM On-Prem can report usage to the correct license pool in CSSM.

a. Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 133

b. Validating Devices (SSM On-Prem UI), on page 133

Note If your product instance is in a NAT set-up, also enable support for a NAT Setup when you enable device validation – both toggle switches are in the same window.

3. ***Product Instance Configuration***

   Where tasks are performed: Product Instance and the SSM On-Prem UI

   Remember to save any configuration changes on the product instance, by entering the **copy running-config startup-config** command in privileged EXEC mode.

   a. Ensuring Network Reachability for Product Instance-Initiated Communication, on page 134

   b. Retrieving the Transport URL (SSM On-Prem UI), on page 137

   c. Setting the Transport Type, URL, and Reporting Interval, on page 159

   The transport type configuration for CSLU and SSM On-Prem are the same (**license smart transport cslu** command in global configuration mode), but the URLs are different.

4. ***Initial Usage Synchronization***

   Where tasks are performed: Product instance, SSM On-Prem, CSSM

   a. Synchronize the product instance with SSM On-Prem.

   On the product instance, enter the **license smart sync** {**all** | **local**} command, in privileged EXEC mode. This synchronizes the product instance with SSM On-Prem, to send and receive any pending data. For example:

   ```
   Device# license smart sync local
   ```

   You can verify this in the SSM On-Prem UI. Log in and select the **Smart Licensing** workspace. Navigate to the **Inventory** > **SL Using Policy** tab. In the **Alerts** column of the corresponding product instance, the following message is displayed: Usage report from product instance.

Note If you have not performed Step 2 above (Addition and Validation of Product Instances), completing this sub-step will add the product instance to the SSM On-Prem database.

b. Synchronize usage information with CSSM (*choose one*):

- Option 1:

  SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.

- Option 2:

  SSM On-Prem is not connected to CSSM: See Exporting and Importing Usage Data (SSM On-Prem UI), on page 137.

Result:

You have completed initial usage synchronization. Product instance and license usage information is now displayed in SSM On-Prem.

For subsequent reporting, you have the following options:

- To synchronize data between the product instance and SSM On-Prem:

  Schedule periodic synchronization between the product instance and the SSM On-Prem, by configuring the reporting interval. Enter the **license smart usage interval** *interval_in_days* command in global configuration mode.

  In the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and all subsequent releases from Cisco IOS XE Cupertino 17.9.1 onwards: The product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and CSSM, by entering the **license smart sync** command in privileged EXEC mode.

  To know when the product instance will be sending the next RUM report, enter the **show license all** command in privileged EXEC mode and in the output, check the `Next report push:` field.

- To synchronize usage information with CSSM schedule periodic synchronization, or , upload and download the required files:

  - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**. Enter the following frequency information and save:

    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.

    - **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400) in your local time zone.

  - Upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 137).

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Tasks for SSM On-Prem Instance-Initiated Communication

SSM On-Prem Installation → Product Instance Addition → Product Instance Configuration→ Initial Usage Synchronization

1. ***SSM On-Prem Installation***

   Where task is performed: A physical server such as a Cisco UCS C220 M3 Rack Server, or a hardware-based server that meets the necessary requirements.

   Download the file from Smart Software Manager > **Smart Software Manager On-Prem**.

   Refer to the *Cisco Smart Software On-Prem Installation Guide* and the *Cisco Smart Software On-Prem User Guide* for help with installation.

   Installation is complete when you have deployed SSM On-Prem, configured a common name on SSM On-Prem (**Security Widget** > **Certificates**), synchronized the NTP server (**Settings** widget > **Time Settings**), and created, registered, and synchronized (**Synchronization** widget) the SSM On-Prem local account with your Smart Account and Virtual Account in CSSM.

   Note Licensing functions in the **On-Prem Licensing Workspace** are greyed-out until you complete the creation, registration, and synchronization of the local account with your Smart Account in CSSM. The *local account* synchronization with CSSM is for the SSM On-Prem instance to be known to CSSM, and is different from usage synchronization which is performed in **4. Initial Usage Synchronization** below.

2. ***Product Instance Addition***

   Where task is performed: SSM On-Prem UI

   Depending on whether you want to add a single product instance or multiple product instances, follow the corresponding sub-steps: Adding One or More Product Instances (SSM On-Prem UI), on page 138.

3. ***Product Instance Configuration***

   Where tasks are performed: Product Instance and the SSM On-Prem UI

   Remember to save any configuration changes on the product instance, by entering the **copy running-config startup-config** command in privileged EXEC mode: Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 139.

4. ***Initial Usage Synchronization***

   Where tasks are performed: SSM On-Prem UI, and CSSM

   a. Retrieve usage information from the product instance.

      In the SSM On-Prem UI, navigate to **Reports** > **Synchronization pull schedule with the devices** > **Synchronize now with the device**.

      In the **Alerts** column, the following message is displayed: Usage report from product instance.

      Tip It takes 60 seconds before synchronization is triggered. To view progress, navigate to the **On-Prem Admin Workspace**, and click the **Support Centre** widget. The system logs here display progress.

   b. Synchronize usage information with CSSM (*choose one*)

- Option 1:

  SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.

- Option 2:

  SSM On-Prem is not connected to CSSM. See: Exporting and Importing Usage Data (SSM On-Prem UI), on page 137.

Result:

You have completed initial usage synchronization. Product instance and license usage information is now displayed in SSM On-Prem. SSM On-Prem automatically sends the ACK back to the product instance. To verify that the product instance has received the ACK, enter the **show license status** command in privileged EXEC mode, and in the output, check the date for the `Last ACK received` field.

For subsequent reporting, you have the following options:

- To retrieve usage information from the product instance, you can:
  - In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
  - Schedule periodic retrieval of information from the product instance by configuring a frequency. In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronization pull schedule with the devices**. Enter values in the following fields:
    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
    - **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400).
  - Collect usage data from the product instance without being connected to CSSM. In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Inventory** > **SL Using Policy** tab. Select one or more product instances by enabling the coresponding check box. Click **Actions for Selected...** > **Collect Usage**. On-Prem connects to the selected Product Instance(s) and collects the usage reports. These usage reports are then stored in On-Prem's local library. These reports can then be transferred to Cisco if On-Prem is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Export/Import All..** > **Export Usage to Cisco**.
- To synchronize usage information with CSSM, you can:
  - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**. Enter the following frequency information and save:
    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
    - **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400).

- Upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 137).

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

Migrating to Smart Licensing Using Policy

To upgrade to Smart Licensing Using Policy, you must upgrade the software version (image) on the product instance to a supported version.

Before you Begin

Ensure that you have read the #unique_104 section, to understand how Smart Licensing Using Policy handles all earlier licensing models.

Smart Licensing Using Policy is introduced in Cisco IOS XE Amsterdam 17.3.2a. This is therefore the minimum required version for Smart Licensing Using Policy.

Note that all the licenses that you are using prior to migration will be available after upgrade. This means that not only registered and authorized licenses (including reserved licenses), but also evaluation licenses will be migrated. The advantage with migrating registered and authorized licenses is that you will have fewer configuration steps to complete after migration, because your configuration is retained after upgrade (transport type configuration and configuration for connection to CSSM, all authorization codes). This ensures a smoother transition to the Smart Licensing Using Policy environment.

Device-led conversion is not supported for migration to Smart Licensing Using Policy.

Upgrading the Wireless Controller Software

For information about the upgrade procedure:

- For Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points, see the *Software Upgrade* section in the Cisco Embedded Wireless Controller on Catalyst Access Points Online Help
- For all other supported wireless controllers, see the *System Upgrade* > *Upgrading the Cisco Catalyst 9800 Wireless Controller Software* section of the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide for the required release.

  If you are upgrading a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the conditions for a mandatory ACK starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.

You can use the procedure to upgrade in install mode or ISSU (ISSU only on supported platforms and supported releases)

After Upgrading the Software Version

- Complete topology implementation.

  If a transport mode is available in your pre-upgrade set-up, this is retained after you upgrade. Only in some cases, like with evaluation licenses or with licensing models where the notion of a transport type

does not exist, the default (**cslu**) is applied - in these cases you may have a few more steps to complete before you are set to operate in the Smart Licensing Using Policy environment.

No matter which licensing model you upgrade from, you can change the topology after upgrade.

- Synchronize license usage with CSSM

  No matter which licensing model you are upgrading from and no matter which topology you implement, synchronize your usage information with CSSM. For this you have to follow the reporting method that applies to the topology you implement. This initial synchronization ensures that up-to-date usage information is reflected in CSSM and a custom policy (if available), is applied. The policy that is applicable after this synchronization also indicates subsequent reporting requirements. These rules are also tabled here: How Upgrade Affects Reporting for Existing Licenses, on page 82

Note After initial usage synchronization is completed, reporting is required only if the policy, or, system messages indicate that it is.

Sample Migration Scenarios

Sample migration scenarios have been provided considering the various existing licensing models and licenses. All scenarios provide sample outputs before and after migration, any CSSM Web UI changes to look out for (as an indicator of a successful migration or further action), and how to identify and complete any necessary post-migration steps.

Note For SSM On-Prem, the sequence in which you perform the various upgrade-related activities is crucial. So only for this scenario, the migration sequence has been provided - and not an example.

Example: Smart Licensing to Smart Licensing Using Policy

The following is an example of a Cisco Catalyst 9800-CL Wireless Controller migrating from Smart Licensing to Smart Licensing Using Policy.

- #unique_178 unique_178_Connect_42_table_l1p_yvl_knb
- #unique_178 unique_178_Connect_42_section_wgh_yvl_knb
- #unique_178 unique_178_Connect_42_section_crc_yvl_knb

The **show** command outputs below call-out key fields to check, before and after migration.

Table 8: Smart Licensing to Smart Licensing Using Policy: show Commands

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)
show license summary The `Status` and `License Authorization` fields show that the license is `REGISTERED` and `AUTHORIZED`.	**show license summary** The `Status` field shows that the licenses are now `IN USE` instead of registered and authorized.

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)

`Device# show license summary`
 	
`Smart Licensing is ENABLED`
 	
`Registration:`
`  Status: REGISTERED`
`  Smart Account: SA-Eg-Company-02`
`  Virtual Account: Dept-02`
`  Export-Controlled Functionality: ALLOWED`
`  Last Renewal Attempt: None`
`  Next Renewal Attempt: May 01 08:19:02 2021 IST`
 	
`License Authorization:`
`  Status: AUTHORIZED`
`  Last Communication Attempt: SUCCEEDED`
`  Next Communication Attempt: Dec 02 08:19:09 2020 IST`
 	
`License Usage:`
`  License  Entitlement tag  Count Status`
`---`
`  AP Perpetual Network... (DNA_NWSTACK_E)  1 AUTHORIZED`
`  Aironet DNA Essentia... (AIR-DNA-E)  1 AUTHORIZED`
	`Device# show license summary`
	
	`License Usage:`
	`  License  Entitlement Tag  Count Status`
	`---`
	`  air-network-essentials  (DNA_NWSTACK_E)  1 IN USE`
	`  air-dna-essentials  (AIR-DNA-E)  1 IN USE`

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)
show license usage One perpetual and one subscription license are being used before upgrade.	**show license usage** All licenses are migrated and the `Enforcement Type` field displays NOT ENFORCED. There are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers.

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)

Device# **show license usage**
 	
License Authorization:
  Status: AUTHORIZED on Nov 02 08:21:29 2020 IST
 	
AP Perpetual Networkstack Essentials (DNA_NWSTACK_E):
  Description: AP Perpetual Network Stack entitled with DNA-E
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
 	
Aironet DNA Essentials Term Licenses (AIR-DNA-E):
  Description: DNA Essentials for Wireless
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
	Device# **show license usage**
	
	License Authorization:
	  Status: Not Applicable
	
	air-network-essentials (DNA_NWSTACK_E):
	  Description: air-network-essentials
	  Count: 1
	  Version: 1.0
	  Status: IN USE
	  Export status: NOT RESTRICTED
	  Feature Name: air-network-essentials
	  Feature Description: air-network-essentials
	  Enforcement type: NOT ENFORCED
	  License type: Perpetual
	
	air-dna-essentials (AIR-DNA-E):
	  Description: air-dna-essentials
	  Count: 1
	  Version: 1.0
	  Status: IN USE
	  Export status: NOT RESTRICTED
	  Feature Name: air-dna-essentials
	  Feature Description: air-dna-essentials
	  Enforcement type: NOT ENFORCED
	  License type: Perpetual

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)
show license status	**show license status** The `Transport:` field shows that the transport type, which was configured before update, is retained after upgrade. The `Policy:` header and details show that a custom policy was available in the Smart Account or Virtual Account – this has also been automatically installed on the product instance. (After establishing trust, CSSM returns a policy. The policy is then automatically installed.) The `Usage Reporting:` header: The `Next report push:` field provides information about when the product instance will send the next RUM report to CSSM. The `Trust Code Installed:` field shows that the ID token is successfully converted and a trusted connected has been established with CSSM.

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)

Device# **show license status**
 	
Smart Licensing is ENABLED
 	
Utility:
  Status: DISABLED
 	
Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED
 	
Transport:
  Type: Callhome
 	
Registration:
  Status: REGISTERED
  Smart Account: SA-Eg-Company-02
  Virtual Account: Dept-02
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 02 08:19:02 2020 IST
  Last Renewal Attempt: None
  Next Renewal Attempt: May 01 08:19:01 2021 IST
  Registration Expires: Nov 02 08:14:06 2021 IST
 	
License Authorization:
  Status: AUTHORIZED on Nov 02 08:21:29 2020 IST
  Last Communication Attempt: SUCCEEDED on Nov 02 08:21:29 2020 IST
  Next Communication Attempt: Dec 02 08:19:09 2020 IST
  Communication Deadline: Jan 31 08:14:15 2021 IST
 	
Export Authorization Key:
  Features Authorized:
  <none>
	Device# **show license status**
	Utility:
	  Status: DISABLED
	
	Smart Licensing Using Policy:
	  Status: ENABLED
	
	Data Privacy:
	  Sending Hostname: yes
	  Callhome hostname privacy: DISABLED
	  Smart Licensing hostname privacy: DISABLED
	  Version privacy: DISABLED
	
	Transport:
	  Type: Callhome
	
	Policy:
	  Policy in use: Installed On Nov 02 09:09:47 2020 IST
	  Policy name: **SLE Policy**
	  Reporting ACK required: yes (Customer Policy)
	  Unenforced/Non-Export Perpetual Attributes:
	  First report requirement (days): 60 (Customer Policy)
	  Reporting frequency (days): 60 (Customer Policy)
	  Report on change (days): 60 (Customer Policy)
	  Unenforced/Non-Export Subscription Attributes:
	  First report requirement (days): 30 (Customer Policy)
	  Reporting frequency (days): 30 (Customer Policy)
	  Report on change (days): 30 (Customer Policy)
	  Enforced (Perpetual/Subscription) License Attributes:
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 90 (Customer Policy)
	  Report on change (days): 90 (Customer Policy)
	  Export (Perpetual/Subscription) License Attributes:
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 90 (Customer Policy)
	  Report on change (days): 90 (Customer Policy)
	
	Miscellaneous:
	  Custom Id: <empty>
	
	Usage Reporting:
	  Last ACK received: Nov 02 09:09:47 2020 IST
	  Next ACK deadline: Jan 01 09:09:47 2021 IST
	  Reporting push interval: 30 days
	  Next ACK push check: Nov 02 09:13:54 2020 IST
	  Next report push: Dec 02 09:05:45 2020 IST
	  Last report push: Nov 02 09:05:45 2020 IST
	  Last report file write: <none>
	
	Trust Code Installed:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	  INSTALLED on Nov 02 08:59:26 2020 IST
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	  INSTALLED on Nov 02 09:00:45 2020 IST

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)
show license udi	**show license udi** This is a High Availability set-up and the command displays all UDIs in the set-up. There is no change in the sample output before and after migration.

`Device# show license udi`
`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
 	
`HA UDI List:`
`Active:PID:C9800-CL-K9,SN:93BBAH93MGS`
`Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`Device# show license udi`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	
	`HA UDI List:`
	`Active:PID:C9800-CL-K9,SN:93BBAH93MGS`
	`Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN`

The CSSM Web UI After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. Under **Inventory** > **Product Instances**.

The product instance previously displayed with the host name (Catalyst 9800CL Cloud Wireless Controller in this example) is now displayed with the UDI instead. All migrated UDIs are displayed, that is, PID:C9800-CL-K9,SN:93BBAH93MGS, and PID:C9800-CL-K9,SN:9XECPSUU4XN.

Only the active product instance reports usage, therefore, PID:C9800-CL-K9,SN:93BBAH93MGS displays license consumption information under **License Usage**. The standby does not report usage and the **License Usage** for the standby displays No Records Found.

Figure 8: Smart Licensing to Smart Licensing Using Policy: Hostname of Product Instance on the CSSM Web UI Before Migration

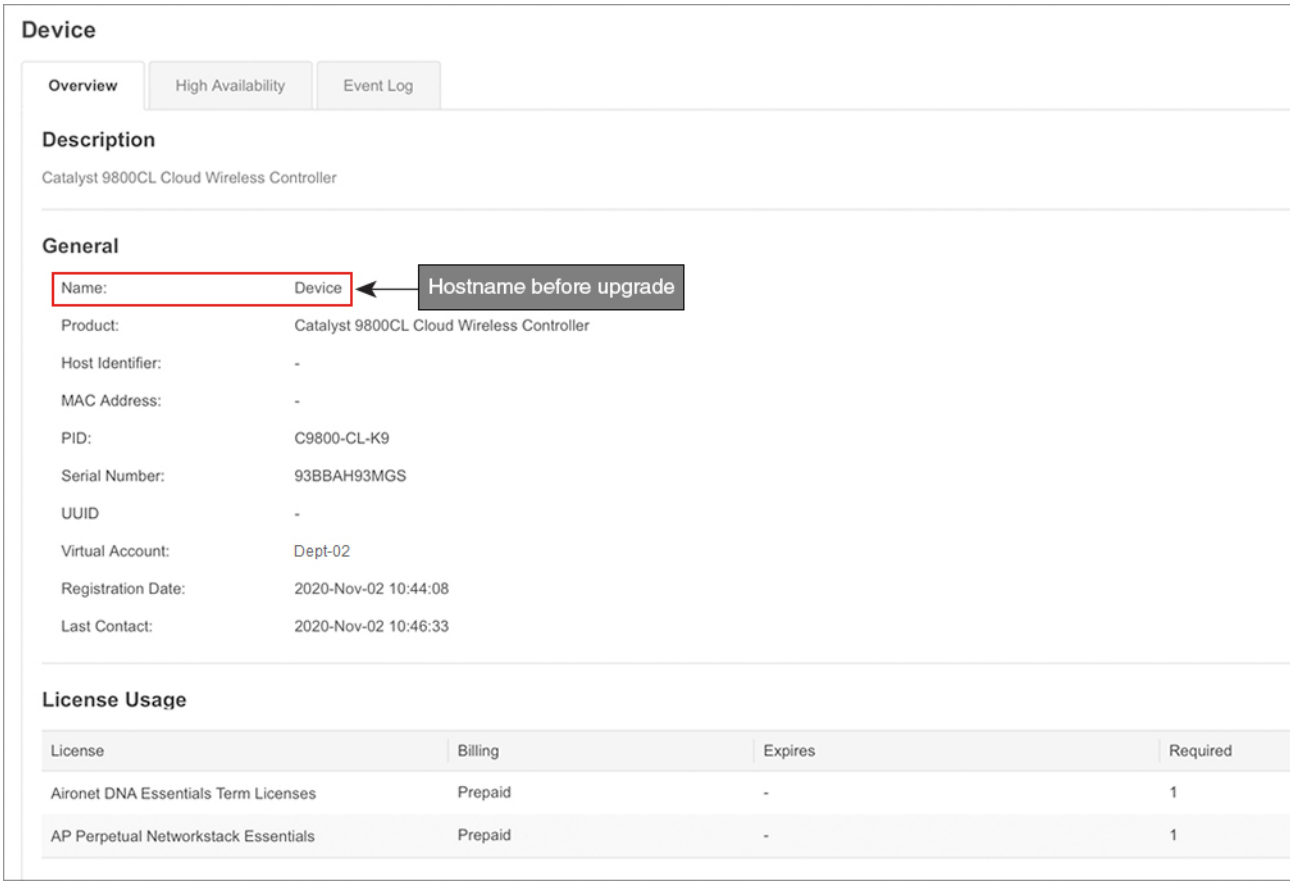


Figure 9: Smart Licensing to Smart Licensing Using Policy: UDI and License Usage Under Active Product Instance After Migration

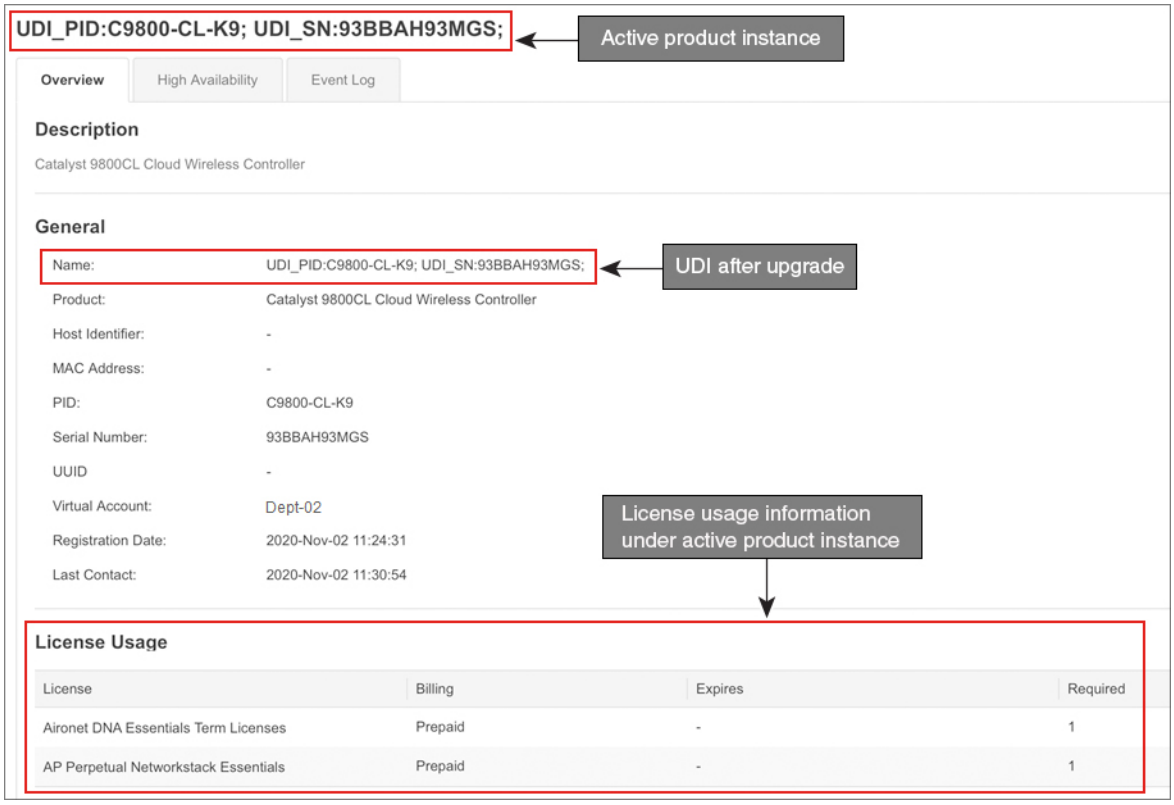
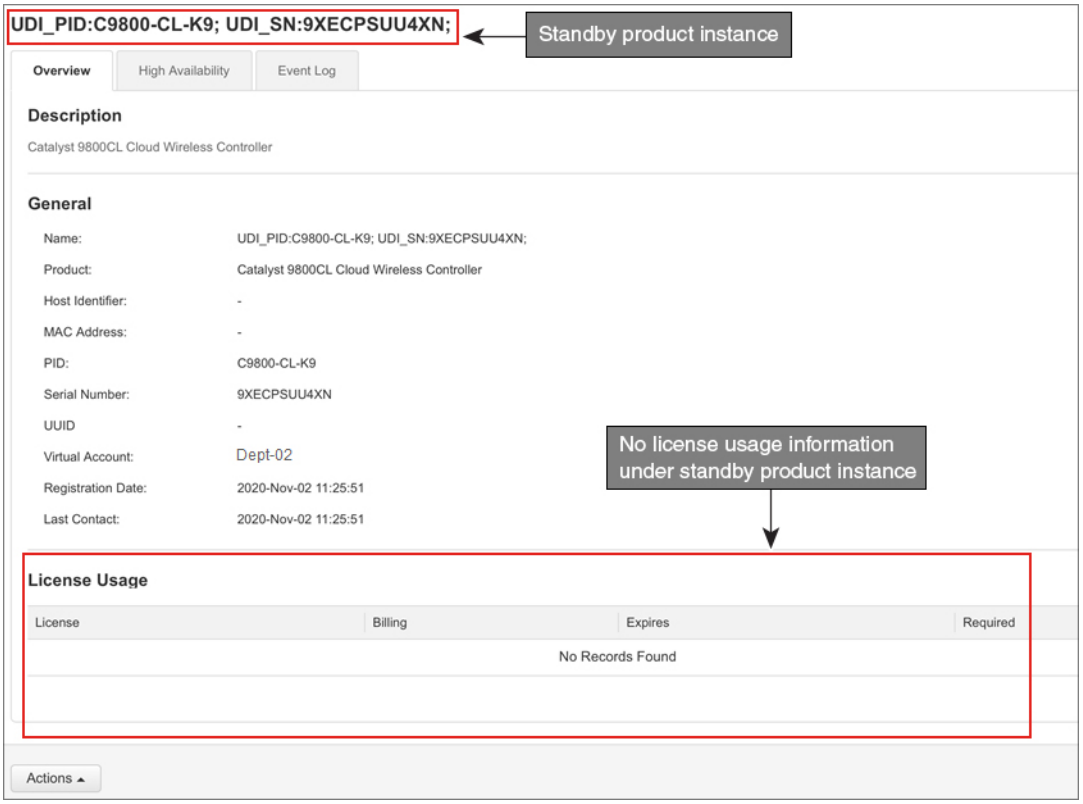


Figure 10: Smart Licensing to Smart Licensing Using Policy: Standby Product Instance After Migration



It is always the active that reports usage, so if the active in this High Availability set-up changes, the new active product instance will display license consumption information and report usage.

Reporting After Migration

The product instance sends the next RUM report to CSSM, based on the policy.

If you want to change your reporting interval to report more frequently: on the product instance, configure the **license smart usage interval** command in global configuration mode. For syntax details see the *license smart (global config)* command in the Command Reference for the corresponding release.

Example: SLR to Smart Licensing Using Policy

The following is an example of a Cisco Catalyst 9800-CL Wireless Controller migrating from Specific License Reservation (SLR) to Smart Licensing Using Policy. This is a High Availability set-up with an active and standby.

License conversion is automatic and authorization codes are migrated. No further action is required to complete migration. After migration the #unique_103 topology is effective. For information about the SLR authorization code in the Smart Licensing Using Policy environment, see #unique_180.

- #unique_181 unique_181_Connect_42_table_dsr_wtl_knb
- #unique_181 unique_181_Connect_42_section_n1l_xtl_knb
- #unique_181 unique_181_Connect_42_section_oqy_wtl_knb

The **show** command outputs below call-out key fields to check, before and after migration.

Table 9: SLR to Smart Licensing Using Policy: show Commands

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

show license summary
The `Registration` and `License Authorization` status fields show that the license was `REGISTERED - SPECIFIC LICENSE RESERVATION` and `AUTHORIZED - RESERVED`.
`Device# show license summary`
`Smart Licensing is ENABLED`
`License Reservation is ENABLED`
`Registration:`
`  Status: REGISTERED - SPECIFIC LICENSE RESERVATION`
`  Export-Controlled Functionality: ALLOWED`
`License Authorization:`
`  Status: AUTHORIZED - RESERVED`
`License Usage:`
`  License  Entitlement tag  Count Status`
`---`
`  AP Perpetual Network... (DNA_NWStack) 1 AUTHORIZED`
`  Aironet DNA Advantag... (AIR-DNA-A) 1 AUTHORIZED`
	show license summary
	Licenses are migrated , but none of the APs have joined the controller, current consumption (Count) is therefore zero, and the `Status` field shows that the licenses are `NOT IN USE`.
	`Device# show license summary`
	`License Reservation is ENABLED`
	`License Usage:`
	`  License  Entitlement Tag  Count Status`
	`---`
	`  Aironet DNA Advantag... (AIR-DNA-A) 0 NOT IN USE`
	`  AP Perpetual Network... (DNA_NWStack) 0 NOT IN USE`

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)
show license reservation	**show license authorization** The `Last Confirmation code:` field shows that the SLR authorization code is successfully migrated for the active and standby product instances in the High Availability set-up. The `Specified license reservations:` header shows that a perpetual license (AP Perpetual Networkstack Advantage) and a subscription license (Aironet DNA Advantage Term Licenses) are the migrated SLR licenses.

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

```
Device# show license reservation
License reservation: ENABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
       Reservation status: SPECIFIC INSTALLED on Nov 02
 03:16:01 2020 IST
       Export-Controlled Functionality: ALLOWED
       Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
       Reservation status: SPECIFIC INSTALLED on Nov 02
 03:15:45 2020 IST
       Export-Controlled Functionality: ALLOWED
       Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled
with DNA-A
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
```

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

	Device# **show license authorization**
	Overall status:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	  Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
	  Last Confirmation code: 102fc949
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	  Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  Last Confirmation code: ad4382fe
	
	Specified license reservations:
	  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
	  Description: DNA Advantage for Wireless
	  Total reserved count: 20
	  Enforcement type: NOT ENFORCED
	  Term information:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-OCT-14 UTC
	  End Date: 2021-APR-12 UTC
	  Term Count: 5
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-JUN-18 UTC
	  End Date: 2020-DEC-15 UTC
	  Term Count: 5
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-OCT-14 UTC
	  End Date: 2021-APR-12 UTC
	  Term Count: 10
	  AP Perpetual Networkstack Advantage (DNA_NWStack):
	  Description: AP Perpetual Network Stack entitled with DNA-A
	  Total reserved count: 20
	  Enforcement type: NOT ENFORCED
	  Term information:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-OCT-14 UTC
	  End Date: 2021-APR-12 UTC
	  Term Count: 5
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-JUN-18 UTC
	  End Date: 2020-DEC-15 UTC
	  Term Count: 5
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
	  License type: TERM
	  Start Date: 2020-OCT-14 UTC
	  End Date: 2021-APR-12 UTC

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

	`Term Count: 10`
	
	`Purchased Licenses:`
	`No Purchase Information Available`

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)
show license status	**show license status** Under the `Transport:` header, the `Type:` field displays that the transport type is set to off. Under the `Usage Reporting:` header, the `Next report push:` field displays if and when the next RUM report must be uploaded to CSSM.

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

-	Device# **show license status**
	
	Utility:
	  Status: DISABLED
	
	Smart Licensing Using Policy:
	  Status: ENABLED
	
	Data Privacy:
	  Sending Hostname: yes
	  Callhome hostname privacy: DISABLED
	  Smart Licensing hostname privacy: DISABLED
	  Version privacy: DISABLED
	
	Transport:
	  Type: Transport Off
	
	Policy:
	  Policy in use: Merged from multiple sources.
	  Reporting ACK required: yes (CISCO default)
	  Unenforced/Non-Export Perpetual Attributes:
	  First report requirement (days): 365 (CISCO default)
	
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 90 (CISCO default)
	  Unenforced/Non-Export Subscription Attributes:
	  First report requirement (days): 90 (CISCO default)
	
	  Reporting frequency (days): 90 (CISCO default)
	  Report on change (days): 90 (CISCO default)
	  Enforced (Perpetual/Subscription) License Attributes:
	
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 0 (CISCO default)
	  Export (Perpetual/Subscription) License Attributes:
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 0 (CISCO default)
	
	Miscellaneous:
	  Custom Id: <empty>
	
	Usage Reporting:
	  Last ACK received: <none>
	  Next ACK deadline: <none>
	  Reporting push interval: 0 (no reporting)
	  Next ACK push check: Nov 01 20:31:46 2020 IST
	  Next report push: <none>
	  Last report push: <none>
	  Last report file write: <none>
	
	Trust Code Installed: <none>

The CSSM Web UI After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. Under **Inventory** > **Product Instances**.

There are no changes in the **Product Instances** tab. The Last Contact column displays "Reserved Licenses" since there has been no usage reporting yet. After the requisite RUM report is uploaded and acknowledged "Reserved Licenses" is no longer displayed and license usage is displayed only in the active product instance.

Figure 11: SLR to Smart Licensing Using Policy: Active Product Instance Before Upgrade

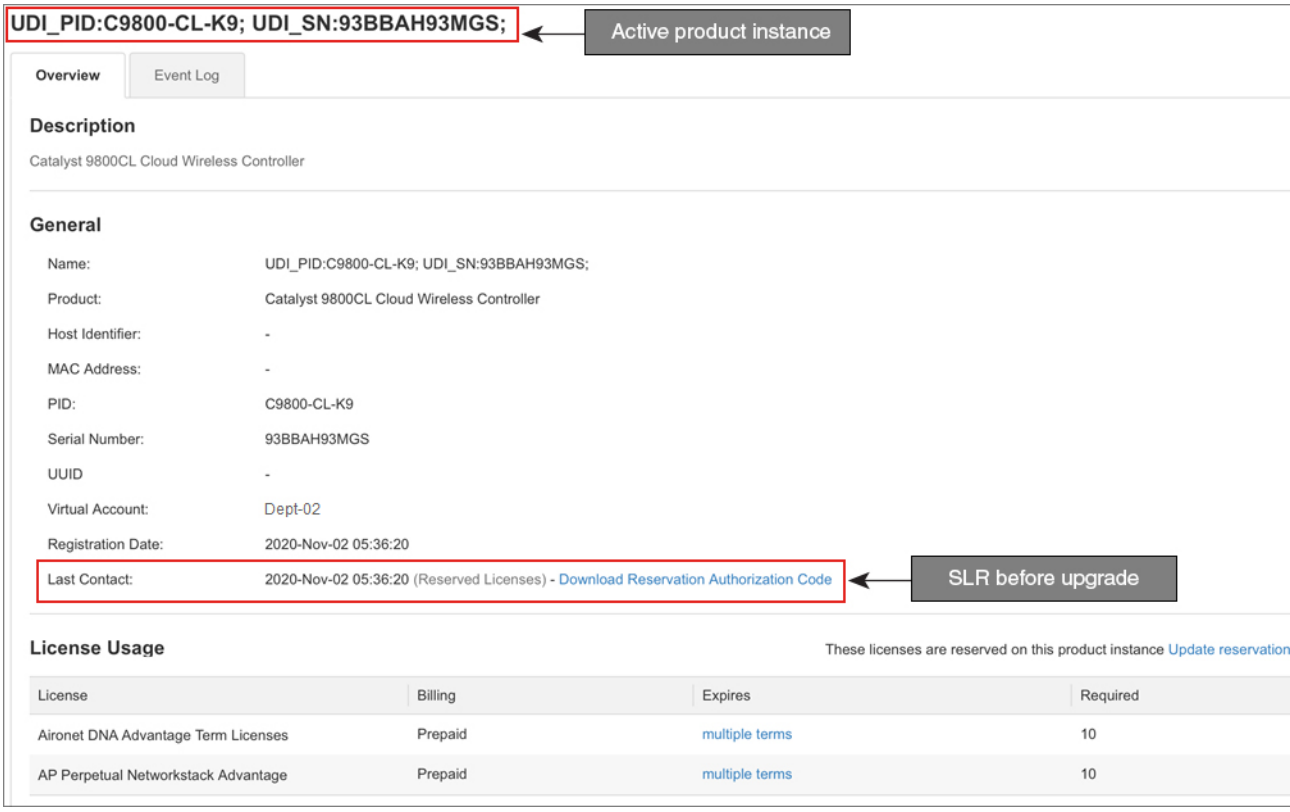
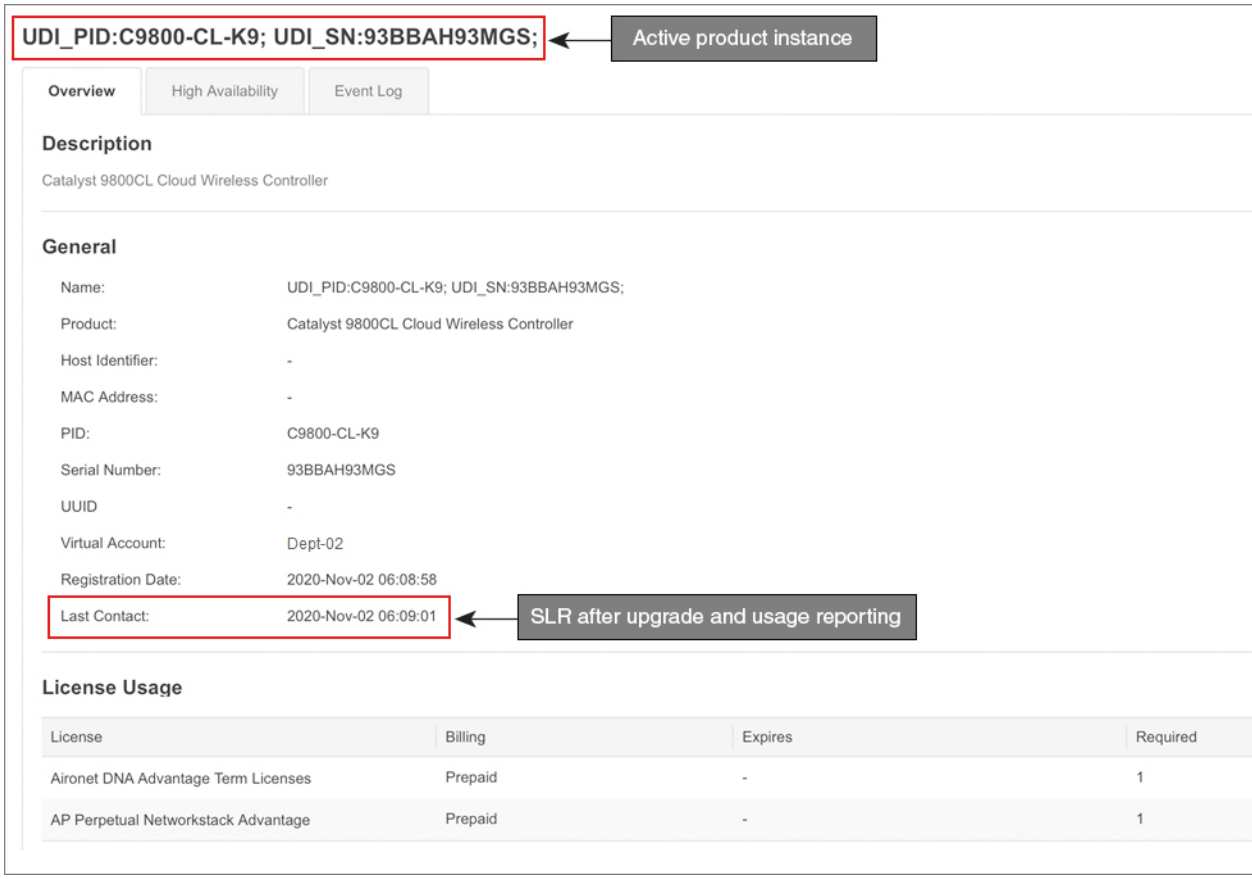


Figure 12: SLR to Smart Licensing Using Policy: Active Product Instance After Upgrade



Reporting After Migration

SLR licenses require reporting only when there is a change in license consumption (For example, when using a subscription license which is for specified term).

In an air-gapped network, use the `Next report push:` date in the **show license status** output to know when the next usage report must be sent. This ensures that the product instance and CSSM are synchronized.

Since all communication to and from the product instance is disabled, to report license usage you must save RUM reports to a file and upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco):

1. Generate and save RUM reports

   Enter the **license smart save usage** command in privileged EXEC mode. In the example below, all RUM reports are saved to the flash memory of the product instance, in file `all_rum.txt`. For syntax details see the *license smart (privileged EXEC)* command in the Command Reference. In the example, the file is first saved to bootflash and then copied to a TFTP location:

   ```
   Device# license smart save usage all bootflash:all_rum.txt
   Device# copy bootflash:all_rum.txt tftp://10.8.0.6/all_rum.txt
   ```

2. Upload usage data to CSSM: #unique_161

3. Install the ACK on the product instance: #unique_164

Example: Evaluation or Expired to Smart Licensing Using Policy

The following is an example of a Cisco Catalyst 9800-CL Wireless Controller with evaluation expired licenses (Smart Licensing) that are migrated to Smart Licensing Using Policy.

The notion of evaluation licenses does not apply to Smart Licensing Using Policy. When the software version is upgraded to one that supports Smart Licensing Using Policy, all licenses are displayed as IN USE and the Cisco default policy is applied to the product instance. Since all licenses on Cisco Catalyst Wireless Controllers are unenforced (enforcement type), no functionality is lost.

- #unique_183 unique_183_Connect_42_table_hdp_4tl_knb
- #unique_183 unique_183_Connect_42_section_qfh_3wl_knb
- #unique_183 unique_183_Connect_42_section_y12_ptl_knb

The table below calls out key changes or new fields to check for in the **show** command outputs, after upgrade to Smart Licensing Using Policy

Table 10: Evaluation or Expired to Smart Licensing Using Policy: show Commands

Before Upgrade (Smart Licensing, Evaluation Mode)	After Upgrade (Smart Licensing Using Policy)

show license summary
Licenses are UNREGISTERED and in `EVAL MODE`.
 	
`Device# show license summary`
`Smart Licensing is ENABLED`
 	
`Registration:`
`  Status: UNREGISTERED`
`  Export-Controlled Functionality: NOT ALLOWED`
 	
`License Authorization:`
`  Status: EVAL EXPIRED`
 	
`License Usage:`
`  License  Entitlement tag  Count Status`
 	
`----------`
 	
`  (DNA_NWStack)  1 EVAL EXPIRED`
`  (AIR-DNA-A)  1 EVAL EXPIRED`
	show license summary
	All licenses are migrated and `IN USE`. There are no EVAL MODE licenses.
	
	`Device# show license summary`
	`License Usage:`
	`  License  Entitlement Tag  Count Status`
	
	`----------`
	
	`  air-network-advantage  (DNA_NWStack)  1 IN USE`
	`  air-dna-advantage  (AIR-DNA-A)  1 IN USE`

Before Upgrade (Smart Licensing, Evaluation Mode)	After Upgrade (Smart Licensing Using Policy)
show license usage	**show license usage** The `Enforcement Type` field displays NOT ENFORCED. (There are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers).

Before Upgrade (Smart Licensing, Evaluation Mode)	After Upgrade (Smart Licensing Using Policy)

`Device# show license usage`
`License Authorization:`
`  Status: EVAL EXPIRED on Apr 14 18:20:46 2020 UTC`
 	
`(DNA_NWStack):`
`  Description:`
`  Count: 1`
`  Version: 1.0`
`  Status: EVAL EXPIRED`
`  Export status: NOT RESTRICTED`
 	
`(AIR-DNA-A):`
`  Description:`
`  Count: 1`
`  Version: 1.0`
`  Status: EVAL EXPIRED`
`  Export status: NOT RESTRICTED`
	`Device# show license usage`
	`License Authorization:`
	`  Status: Not Applicable`
	
	`air-network-advantage (DNA_NWStack):`
	`  Description: air-network-advantage`
	`  Count: 1`
	`  Version: 1.0`
	`  Status: IN USE`
	`  Export status: NOT RESTRICTED`
	`  Feature Name: air-network-advantage`
	`  Feature Description: air-network-advantage`
	`  Enforcement type: NOT ENFORCED`
	`  License type: Perpetual`
	
	`air-dna-advantage (AIR-DNA-A):`
	`  Description: air-dna-advantage`
	`  Count: 1`
	`  Version: 1.0`
	`  Status: IN USE`
	`  Export status: NOT RESTRICTED`
	`  Feature Name: air-dna-advantage`
	`  Feature Description: air-dna-advantage`
	`  Enforcement type: NOT ENFORCED`
	`  License type: Perpetual`

Before Upgrade (Smart Licensing, Evaluation Mode)	After Upgrade (Smart Licensing Using Policy)
show license status	**show license status** The `Transport:` field displays that the default type is set, but a URL or a method for the product instance to discover CSLU is not specified. The `Trust Code Installed:` field displays that a trust code is not installed. The `Policy:` header and details show that the `Cisco default` policy is applied. Under the `Usage Reporting:` header, the `Next report push:` field provides information about when the next RUM report must be sent to CSSM.

Before Upgrade (Smart Licensing, Evaluation Mode)	After Upgrade (Smart Licensing Using Policy)

Device# **show license status**
 	
Smart Licensing is ENABLED
 	
Utility:
  Status: DISABLED
 	
Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED
 	
Transport:
  Type: Callhome
 	
Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED
 	
License Authorization:
  Status: EVAL EXPIRED on Apr 14 18:20:46 2020 UTC
 	
Export Authorization Key:
  Features Authorized:
  <none>
	Device# **show license status**
	Utility:
	  Status: DISABLED
	
	Smart Licensing Using Policy:
	  Status: ENABLED
	
	Data Privacy:
	  Sending Hostname: yes
	  Callhome hostname privacy: DISABLED
	  Smart Licensing hostname privacy: DISABLED
	  Version privacy: DISABLED
	
	Transport:
	  Type: cslu
	  Cslu address: <empty>
	  Proxy:
	  Not Configured
	
	Policy:
	  Policy in use: Merged from multiple sources.
	  Reporting ACK required: yes (CISCO default)
	  Unenforced/Non-Export Perpetual Attributes:
	  First report requirement (days): 365 (CISCO default)
	
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 90 (CISCO default)
	  Unenforced/Non-Export Subscription Attributes:
	  First report requirement (days): 90 (CISCO default)
	
	  Reporting frequency (days): 90 (CISCO default)
	  Report on change (days): 90 (CISCO default)
	  Enforced (Perpetual/Subscription) License Attributes:
	
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 0 (CISCO default)
	  Export (Perpetual/Subscription) License Attributes:
	  First report requirement (days): 0 (CISCO default)
	  Reporting frequency (days): 0 (CISCO default)
	  Report on change (days): 0 (CISCO default)
	
	Miscellaneous:
	  Custom Id: <empty>
	
	Usage Reporting:
	  Last ACK received: <none>
	  Next ACK deadline: <none>
	  Reporting push interval: 0 (no reporting)
	  Next ACK push check: <none>
	  Next report push: <none>
	  Last report push: <none>
	  Last report file write: <none>
	
	Trust Code Installed: <none>

The CSSM Web UI After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. Under **Inventory** > **Product Instances**, the Last Contact field for the migrated product instances display an updated timestamp after migration.

Reporting After Migration

Implement any one of the supported topologies, and fulfil reporting requirements. See #unique_96 and #unique_114. The reporting method you can use depends on the topology you implement.

Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy

If you are using a version of SSM On-Prem that is earlier than the minimum required version (See SSM On-Prem, on page 63), you can use this section as an outline of the process and sequence you have to follow to migrate the SSM On-Prem version and the product instance.

1. Upgrade SSM On-Prem.

   Upgrade to the minimum required Version 8, Release 202102 or a later version.

   Refer to the Cisco Smart Software Manager On-Prem Migration Guide.

2. Upgrade the product instance.

   For information about the minimum required software version, see SSM On-Prem, on page 63.

   For information about the upgrade procedure, see #unique_115 unique_115_Connect_42_section_ixm_qty_jqb.

3. Re-Register a local account with CSSM

   Online and Offline options are available. Refer to the Cisco Smart Software Manager On-Prem Migration Guide > *Re-Registering a local Account (Online Mode)* or *Manually Re-Registering a Local Account (Offline Mode)* .

   Once re-registration is complete, the following events occur automatically:

   - SSM On-Prem responds with new transport URL that points to the tenant in SSM On-Prem.
   - The transport type configuration on the product instance changes from **call-home** or **smart**, to **cslu**. The transport URL is also updated automatically.

4. Save configuration changes on the product instance, by entering the **copy running-config startup-config** command in privileged EXEC mode.

5. Clear older On-Prem Smart Licensing certificates on the product instance and reload the product instance. Do not save configuration changes after this.

Note This step is required only if the software version running on the product instance is Cisco IOS XE Amsterdam 17.3.x or Cisco IOS XE Bengaluru 17.4.x.

   Enter the **license smart factory reset** and then the **reload** commands in privileged EXEC mode.

```
Device# license smart factory reset
Device# reload
```

6. Perform usage synchronization

   a. On the product instance, enter the **license smart sync** {**all**|**local**} command, in privileged EXEC mode. This synchronizes the product instance with SSM On-Prem, to send and receive any pending data.

      ```
      Device(config)# license smart sync local
      ```

      You can verify this in the SSM On-Prem UI. Go to **Inventory** > **SL Using Policy**. In the **Alerts** column, the following message is displayed: Usage report from product instance.

   b. Synchronize usage information with CSSM (*choose one*)

      - Option 1:

        SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.

      - Option 2:

        SSM On-Prem is not connected to CSSM. See Exporting and Importing Usage Data (SSM On-Prem UI), on page 137.

Result:

You have completed migration and initial usage synchronization. Product instance and license usage information is now displayed in SSM On-Prem.

For subsequent reporting, you have the following options:

- To synchronize data between the product instance and SSM On-Prem:
  - Schedule periodic synchronization between the product instance and SSM On-Prem, by configuring the reporting interval. Enter the **license smart usage interval** *interval_in_days* command in global configuration mode.

    To know when the product instance will be sending the next RUM report, enter the **show license all** command in privileged EXEC mode and in the output, check the `Next report push:` field.

  - Enter the **license smart sync** privileged EXEC command, for ad hoc or on-demand synchronization between the product instance and SSM On-Prem.

- To synchronize usage information with CSSM:
  - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**. Enter the following frequency information and save:
    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
    - **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400) in your local time zone.

- Upload and download the required files for reporting. See Exporting and Importing Usage Data (SSM On-Prem UI), on page 137.

Task Library for Smart Licensing Using Policy

This section is a grouping of tasks that apply to Smart Licensing Using Policy. It includes tasks performed on a product instance, on the CSLU interface, and on the CSSM Web UI.

To implement a particular topology, refer to the corresponding workflow to know the sequential order of tasks that apply. See #unique_114.

To perform any additional configuration tasks, for instance, to configure a different license, or use an add-on license, or to configure a narrower reporting interval, refer to the corresponding task here. Check the "Supported Topologies" where provided, before you proceed.

RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller

About This Requirement

Beginning with Cisco IOS XE Cupertino 17.7.1, if you are using a *Cisco Catalyst 9800-CL Wireless Controller*, you must complete RUM (Resource Utilization Measurement) reporting and ensure that the Acknowledgment (ACK) is made available on the product instance - at least once. This is to ensure that correct and up-to-date usage information is reflected in CSSM.

Prior to Cisco IOS XE Cupertino 17.7.1, RUM reporting and ACK installation was not mandatory for a Cisco Catalyst *9800-CL* Wireless Controller (unlike other Cisco Catalyst Wireless Controllers).

This requirement is applicable to:

- A new Cisco Catalyst 9800-CL Wireless Controller purchased through the Cisco Commerce portal or downloaded from the Software Download page, and where the software version running on the product instance is Cisco IOS XE Cupertino 17.7.1 or a later release.
- An existing Cisco Catalyst 9800-CL Wireless Controller that is upgraded to Cisco IOS XE Cupertino 17.7.1 or later release.

Required Action to Meet This Requirement

The following procedure provides information about what you have to do to ensure compliance with this requirement and avoid any throttling restrictions on new and upgraded product instances. This procedure is followed by a flow chart which depicts the same information.

1. Check when the ACK is expected. Note system behavior if you don't meet the ACK deadline.

   Enter the **show license air entities summary** command in privileged EXEC mode and check field `License Ack expected within.....: [n] days.`

   System behavior if you do not meet the ACK deadline:

Note If the number of AP joins is greater than 10, the system displays this system message once-a-day until an ACK is installed: %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG.

- *If an ACK is not installed by the ACK deadline, and the count of currently active APs is lesser than or equal to 50*, the system throttles the AP join count to 50.
- *If an ACK is not installed by the ACK deadline and the count of currently active APs is greater than 50*, these currently active APs are not disconnected, but no new AP joins are allowed.
- If there is a reload after the throttled state has come into effect, the system throttles the number of currently active APs to 50 when the system comes up after reload.
- If there is a stateful switchover (SSO) after the throttled state has come into effect, all connected APs remain joined.
- The following system message is displayed when the throttling restriction is effective and a new AP tries to join: %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED.

The AP join restriction and the display of the system messages continues until the first ACK is made available on the product instance.

2. Implement a supported topology.

   If you have not already done so, implement one of the supported topologies and complete usage reporting. The method you use to send the RUM report to CSSM and ACK installation depends on the topology you implement.

   For more information, see: Supported Topologies, on page 69 and How to Configure Smart Licensing Using Policy: Workflows by Topology , on page 86.

3. Ensure that the ACK is available on the product instance.

   In the output of the **show license status** command in privileged EXEC mode check for an updated timestamp in the `Last ACK received:`.

```
Device# show license status
<output truncated>
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>
```

   In the output of the **show license air entities summary** command in privileged EXEC mode, the `License Ack expected within.....: [n] days` field is no longer displayed.

```
Device# show license air entities summary
Upcoming license report time.....: 21:05:16.092 UTC Mon Oct 25 2021
No. of APs active at last report.....: 57
No. of APs newly added with last report.....: 57
No. of APs deleted with last report.....: 0
```

   Once the first ACK is installed, the system messages (%IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG and

%CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED) are not displayed any longer and AP join throttling restrictions are lifted.

Figure 13: Flow Chart of System Events, User Actions, and System Actions on a Cisco Catalyst 9800-CL Wireless Controller

Logging into Cisco (CSLU Interface)

Depending on your needs, when working in CSLU, you can either be in connected or disconnected mode. To work in the connected mode, complete these steps to connect with Cisco.

Procedure

Step 1 From the CSLU Main screen, click **Login to Cisco** (located at the top right corner of the screen).

Step 2 Enter: **CCO User Name** and **CCO Password**.

Step 3 In the CSLU Preferences tab, check that the Cisco connectivity toggle displays “Cisco Is Available”.

Configuring a Smart Account and a Virtual Account (CSLU Interface)

Both the Smart Account and Virtual Account are configured through the Preferences tab. Complete the following steps to configure both Smart and Virtual Accounts for connecting to Cisco.

Procedure

Step 1 Select the **Preferences Tab** from the CSLU home screen.

Step 2 Perform these steps for adding both a Smart Account and Virtual Account:

a) In the Preferences screen navigate to the **Smart Account** field and add the **Smart Account Name**.

b) Next, navigate to the **Virtual Account** field and add the **Virtual Account Name**.

If you are connected to CSSM (In the Preferences tab, **Cisco is Available**), you can select from the list of available SA/VAs.

If you are not connected to CSSM (In the Preferences tab, **Cisco Is Not Available**), enter the SA/VAs manually.

Note SA/VA names are case sensitive.

Step 3 Click **Save**. The SA/VA accounts are saved to the system

Only one SA/VA pair can reside on CSLU at a time. You cannot add multiple accounts. To change to another SA/VA pair, repeat Steps 2a and 2b then Save. A new SA/VA account pair replaces the previous saved pair

Adding a Product-Initiated Product Instance in CSLU (CSLU Interface)

Complete these steps to add a device-created Product Instance using the Preferences tab.

Procedure

Step 1 Select the **Preferences** tab.

Step 2 In the Preferences screen, de-select the **Validate Device** check box.

Step 3 Set the **Default Connect Method** to **Product Instance Initiated** and then click **Save**.

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps my be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (product instance-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface. **Note** Cisco Catalyst 9800-L-F Wireless Controller 10G Ports do not support in an auto-negotiation operation.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 8	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface gigabitethernet0/0`	Configures a source interface for the HTTP client.
Step 9	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	(Required) Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# Device(config)# ip name-server vrf mgmt-vrf 173.37.137.85`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Configures the source interface for the DNS domain lookup. **Note** If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 12	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configure DNS discovery of your domain. In accompanying example, the name-server creates entry `cslu-local.example.com`.

Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface)

Using the CSLU interface, you can configure the connect method to be CSLU Initiated. This connect method (mode) enables CSLU to retrieve Product Instance information from the Product Instance.

Note The default Connect Method is set in the **Preferences** tab.

Complete these steps to add a Product Instance from the Inventory tab

Procedure

Step 1 Go to the **Inventory** tab and from the Product Instances table, select **Add Single Product**.

Step 2 Enter the **Host** (IP address of the Host).

Step 3 Select the **Connect Method** and select one of the CSLU Initiated connect methods.

Step 4 In the right panel, click **Product Instance Login Credentials**. The left panel of the screen changes to show the User Name and Password fields.

Step 5 Enter the product instance **User Name** and **Password**.

Step 6 Click **Save**.

The information is saved to the system and the device is listed in the Product Instances table with the Last Contact listed as never.

Collecting Usage Reports: CSLU Initiated (CSLU Interface)

CSLU also allows you to manually trigger the gathering of usage reports from devices.

After configuring and selecting a product instance (selecting **Add Single Product**, filling in the **Host** name and selecting a CSLU-initiated connect method), click **Actions for Selected** > **Collect Usage**. CSLU connects to the selected product instances and collects the usage reports. These usage reports are stored in CSLU's local library. These reports can then be transferred to Cisco if CSLU is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Data** > **Export to CSSM**.

If you are working in CSLU-initiated mode, complete these steps to configure CSLU to collect RUM reports from Product Instances.

Procedure

Step 1 Click the **Preference** tab and enter a valid **Smart Account** and **Virtual Account**, and then select an appropriate CSLU-initiated collect method. (If there have been any changes in Preferences, make sure you click **Save**).

Step 2 Click the **Inventory** tab and select one or more product instances.

Step 3 Click **Actions for Selected** > **Collect Usage**.

RUM reports are retrieved from each selected device and stored in the CSLU local library. The Last Contacted column is updated to show the time the report was received, and the Alerts column shows the status.

If CSLU is currently logged into Cisco the reports will be automatically sent to the associated Smart Account and Virtual Account in Cisco and Cisco will send an acknowledgement to CSLU as well as to the product instance. The acknowledgement will be listed in the alerts column of the Product Instance table. To manually transfer usage reports Cisco, from the CSLU main screen select **Data** > **Export to CSSM**.

Step 4 From the **Export to CSSM** modal, select the local directory where the reports are to be stored. (<CSLU_WORKING_Directory>/data/default/rum/unsent)

At this point, the usage reports are saved in your local directory (library). To upload these usage reports to Cisco, follow the steps described in #unique_161.

Note The Windows operating system can change the behavior of a usage report file properties by dropping the extension when that file is renamed. The behavior change happens when you rename the downloaded file and the renamed file drops the extension. For example, the downloaded default file named `UD_xxx.tar` is renamed to `UD_yyy`. The file loses its TAR extension and cannot function. To enable the usage file to function normally, after re-naming a usage report file, you must also add the TAR extension back to the file name, for example `UD_yyy.tar`.

Export to CSSM (CSLU Interface)

The Download All for Cisco menu option is a manual process used for offline purposes. Complete these steps to use the Download For Cisco menu option

Procedure

Step 1 Go to the **Preferences** tab, and turn off the **Cisco Connectivity** toggle switch.

The field switches to "Cisco Is Not Available".

Step 2 From the main menu in the CSLU home screen navigate to **Data** > **Export to CSSM**.

Step 3 Select the file from the modal that opens and click **Save**. You now have the file saved.

Note At this point you have a DLC file, RUM file, or both.

Step 4 Go to a station that has connectivity to Cisco, and complete the following: #unique_161

Once the file is downloaded, you can import it into CSLU, see #unique_162.

Import from CSSM (CSLU Interface)

Once you have received the ACK or other file (such as an authorization code) from Cisco, you are ready to Upload that file to your system. This procedure can be used for workstations that are offline. Complete these steps to select and upload files from Cisco.

Procedure

Step 1 Ensure that you have downloaded the file to a location that is accessible to CSLU.

Step 2 From the main menu in the CSLU home screen, navigate to **Data** > **Import from CSSM**.

Step 3 An Import from CSSM modal open for you to either:

- Drag and Drop a file that resides on your local drive, or
- Browse for the appropriate *.xml file, select the file and click **Open**.

If the upload is successful, you will get message indicating that the file was successfully sent to the server. If the upload is not successful, you will get an import error.

Step 4 When you have finished uploading, click the **x** at the top right corner of the modal to close it.

Ensuring Network Reachability for CSLU-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for CSLU-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (CSLU-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new model** **Example:** `Device(config)# aaa new model`	(Required) Enable the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	(Required) Sets AAA authentication to use the local username database for authentication.
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.
Step 6	ip routing **Example:**	Enables IP routing.

	Command or Action	Purpose
	`Device(config)# ip routing`	
Step 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	(Optional) Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 8	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS). **Note** If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 9	**ip domain name** *name* **Example:** `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 10	**no username** *name* **Example:** `Device(config)# no username admin`	(Required) Clears the specified username, if it exists. For *name* , enter the same username you will create in the next step. This ensures that a duplicate of the username you are going to create in the next step does not exist. If you plan to use REST APIs for CSLU-initiated retrieval of RUM reports, you have to log in to CSLU. Duplicate usernames may cause the feature to work incorrectly if there are duplicate usernames in the system.

	Command or Action	Purpose

Step 11	**username** *name* **privilege** *level* **password** *password*
	Example:
	`Device(config)# username admin privilege 15`
	`password 0 lab`
		(Required) Establishes a username-based authentication system.
		The **privilege** keyword sets the privilege level for the user. A number between 0 and 15 that specifies the privilege level for the user.
		The password allows access to the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
		This enables CSLU to use the product instance native REST.
		Note Enter this username and password in CSLU (#unique_151 → *Step 4. f*. CSLU can then collect RUM reports from the product instance.

Step 12	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 13	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 15	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 16	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts a disabled interface.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 18	**ip http server** **Example:** `Device(config)# ip http server`	(Required) Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. The HTTP server uses the standard port 80, by default.

Step 19	**ip http authentication local**
	Example:
	`ip http authentication local`
	`Device(config)#`
		(Required) Specifies a particular authentication method for HTTP server users.
		The **local** keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.

Step 20	**ip http secure-server** **Example:** `Device(config)# ip http server`	(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.
Step 21	**ip http max-connections** **Example:** `Device(config)# ip http max-connections 16`	(Required) Configures the maximum number of concurrent connections allowed for the HTTP server. Enter an integer in the range from 1 to 16. The default is 5.
Step 22	**ip tftp source-interface** *interface-type-number* **Example:** `Device(config)# ip tftp source-interface GigabitEthernet0/0`	Specifies the IP address of an interface as the source address for TFTP connections.
Step 23	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 24	**logging host** **Example:** `Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	Logs system messages and debug output to a remote host.
Step 25	**end** **Example:** `Device(config)# end`	Exits the global configuration mode and enters privileged EXEC mode.
Step 26	**show ip http server session-module** **Example:**	(Required) Verifies HTTP connectivity. In the output, check that `SL_HTTP` is active. Additionally, you can also perform the following checks :

	Command or Action	Purpose
	`Device# show ip http server session-module`	• From device where CSLU is installed, verify that you can ping the product instance. A successful ping confirms that the product instance is reachable. • From a Web browser on the device where CSLU is installed verify `https://<product-instance-ip>/`. This ensures that the REST API from CSLU to the product instance works as expected.

Assigning a Smart Account and Virtual Account (SSM On-Prem UI)

You can use this procedure to import one or more product instances along with corresponding Smart Account and Virtual Account information, into the SSM On-Prem database. This enables SSM On-Prem to map product instances that are part of local virtual accounts (other than the default local virtual account), to the correct license pool in CSSM:

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 Log into the SSM On-Prem and select the **Smart Licensing** workspace.

Step 2 Navigate to **Inventory** > **SL Using Policy** > **Export/Import All** > **Import Product Instances List**

The **Upload Product Instances** window is displayed.

Step 3 Click **Download** to download the .csv template file and enter the required information for all the product instances in the template.

Step 4 Once you have filled-out the template, click **Inventory** > **SL Using Policy** > **Export/Import All** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

Step 5 Now, click **Browse** and upload the filled-out .csv template.

Smart Account and Virtual Account information for all uploaded product instances is now available in SSM On-Prem.

Validating Devices (SSM On-Prem UI)

When device validation is enabled, RUM reports from an unknown product instance (not in the SSM On-Prem database) are rejected.

By default, devices are not validated. Complete the following steps to enable it:

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 In the **On-Prem License Workspace** window, click **Admin Workspace** and log in, if prompted.

The **On-Prem Admin Workspace** window is displayed.

Step 2 Click the **Settings** widget.

The **Settings** window is displayed.

Step 3 Navigate to the **CSLU** tab and turn-on the **Validate Device** toggle switch.

RUM reports from an unknown product instance will now be rejected. If you haven't already, you must now add the required product instances to the SSM On-Prem database before sending RUM reports. See Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 133

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps my be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Note Ensure that you configure steps 13, 14, and 15 exactly as shown below. These commands must be configured to ensure that the correct trustpoint is used and that the necessary certificates are accepted for network reachability.

Before you begin

Supported topologies: SSM On-Prem Deployment(product instance-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 8	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface gigabitethernet0/0`	Configures a source interface for the HTTP client.
Step 9	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	(Required) Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# Device(config)# ip name-server vrf mgmt-vrf 198.51.100.1`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**ip domain lookup source-interface** *interface-type-number* **Example:**	Configures the source interface for the DNS domain lookup.

	Command or Action	Purpose
	`Device(config)# ip domain lookup source-interface gigabitethernet0/0`	**Note** If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 12	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configure DNS discovery of your domain. In the accompanying example, the name-server creates entry `cslu-local.example.com`.

Step 13	**crypto pki trustpoint SLA-TrustPoint**
	Example:
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		(Required) Declares that the product instance should use trustpoint "SLA-TrustPoint" and enters the ca-trustpoint configuration mode. The product instance does not recognize any trustpoints until you declare a trustpoint using this command.

Step 14	enrollment terminal **Example:** `Device(ca-trustpoint)# enrollment terminal`	Required) Specifies the certificate enrollment method.
Step 15	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	(Required) Specifies a method that is to be used to ensure that the certificate of a peer is not revoked. For the SSM On-Prem Deployment topology, enter the **none** keyword. This means that a revocation check will not be performed and the certificate will always be accepted.

Step 16	**exit**
	Example:
	`Device(ca-trustpoint)# exit`
	`Device(config)# exit`
		Exits the ca-trustpoint configuration mode and then the global configuration mode and returns to privileged EXEC mode.

Step 17	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Retrieving the Transport URL (SSM On-Prem UI)

You must configure the transport URL on the product instance when you deploy the product instance-initiated communication with SSM On-Prem deployment. This task show you how to easily copy the complete URL including the tenant ID from SSM On-Prem.

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 Log into SSM On-Prem and select the **Smart Licensing** workspace.

Step 2 Navigate to the **Inventory** tab and from the dropdown list of local virtual accounts (top right corner), select the *default local virtual account*. When you do, the area under the **Inventory** tab displays **Local Virtual Account: Default**.

Step 3 Navigate to the **General** tab.

The **Product Instance Registration Tokens** area is displayed.

Step 4 In the **Product Instance Registration Tokens** area click **CSLU Transport URL**.

The **Product Registration URL** pop-window is displayed.

Step 5 Copy the entire URL and save it in an accessible place.

You will require the URL when you configure the transport type and URL on the product instance.

Step 6 Configure the transport type and URL. See: Setting the Transport Type, URL, and Reporting Interval, on page 159.

Exporting and Importing Usage Data (SSM On-Prem UI)

You can use this procedure to complete usage synchronization between SSM On-Prem and CSSM when SSM On-Prem is disconnected from CSSM.

Before you begin

Supported topologies:

- SSM On-Prem Deployment (SSM On-Prem-initiated communication)
- SSM On-Prem Deployment (product instance-initiated communication).

Reporting data must be available in SSM On-Prem. You must have either pushed the necessary reporting data from the product instance to SSM On-Prem (product instance-initiated communication) or retrieved the necessary reporting data from the product instance (SSM On-Prem-initiated communication).

Procedure

Step 1 Log into SSM On-Prem and select **Smart Licensing**.

Step 2 Navigate to **Inventory** > **SL Using Policy** tab.

Step 3 In the **SL Using Policy** tab area, click **Export/Import All...** > **Export Usage to Cisco**.

This generates one .tar file with *all* the usage reports available in the SSM On-Prem server.

Step 4 Complete this task in CSSM: #unique_161.

At the end of this task you will have an ACK file to import into SSM On-Prem.

Step 5 Again navigate to the **Inventory** > **SL Using Policy** tab.

Step 6 In the **SL Using Policy** tab area, click **Export/Import All...** > **Import From Cisco** . Upload the .tar ACK file.

To verify ACK import, in the **SL Using Policy** tab area check the **Alerts** column of the corresponding product instance. The following message is displayed: Acknowledgement received from CSSM.

Adding One or More Product Instances (SSM On-Prem UI)

You can use this procedure to add one product instance or to import and add multiple product instances. It enables SSM On-Prem to retrieve information from the product instance.

Before you begin

Supported topologies: SSM On-Prem Deployment (SSM On-Prem-initiated communication).

Procedure

Step 1 Log into the SSM On-Prem UI and click **Smart Licensing**.

Step 2 Navigate to **Inventory** tab. Select a local virtual account from the drop-down list in the top right corner.

Step 3 Navigate to the **SL Using Policy** tab.

Step 4 Add a single product or import multiple product instances (*choose one*).

- **To add a single product instance**:
  - **a.** In the **SL Using Policy** tab area, click **Add Single Product**.
  - **b.** In the **Host** field, enter the IP address of the host (product instance).
  - **c.** From the **Connect Method** dropdown list, select an appropriate SSM On-Prem-initiated connect method.

    The available connect methods for SSM On-Prem-initiated communication are: NETCONF, RESTCONF, and REST API.
  - **d.** In the right panel, click **Product Instance Login Credentials**.

    The **Product Instance Login Credentials** window is displayed

Note You need the login credentials only if a product instance requires a SLAC.

e. Enter the **User ID** and **Password**, and click **Save**.

This is the same user ID and password that you configured as part of commands required to establish network reachability (Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 139).

Once validated, the product instance is displayed in the listing in the **SL Using Policy** tab area.

- **To import multiple product instances:**

a. In **SL Using Policy** tab, click **Export/Import All...** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

b. Click **Download** to download the predefined .csv template.

c. Enter the required information for all the product instances in the .csv template.

In the template, ensure that you provide **Host**, **Connect Method** and **Login Credentials** for all product instances.

The available connect methods for SSM On-Prem-initiated communication are: NETCONF, RESTCONF, and REST API.

Login credentials refer to the user ID and password that you configured as part of commands required to establish network reachability (Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 139).

d. Again navigate to **Inventory** > **SL Using Policy** tab. Click **Export/Import All....** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

e. Now upload the filled-out .csv template.

Once validated, the product instances are displayed in the listing in the **SL Using Policy** tab.

Ensuring Network Reachability for SSM On-Prem-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for SSM On-Prem-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Note Ensure that you configure steps 25, 26, and 27 exactly as shown below. These commands must be configured to ensure that the correct trustpoint is used and that the necessary certificates are accepted for network reachability.

Before you begin

Supported topologies: SSM On-Prem Deployment (SSM On-Prem-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new model** **Example:** `Device(config)# aaa new model`	(Required) Enable the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	(Required) Sets AAA authentication to use the local username database for authentication.
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.
Step 6	ip routing **Example:** `Device(config)# ip routing`	Enables IP routing.
Step 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	(Optional) Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 8	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not

	Command or Action	Purpose
		control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS). **Note** If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 9	**ip domain name** *name* **Example:** `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 10	**no username** *name* **Example:** `Device(config)# no username admin`	(Required) Clears the specified username, if it exists. For *name* , enter the same username you will create in the next step. This ensures that a duplicate of the username you are going to create in the next step does not exist. If you plan to use REST APIs for SSM On-Prem-initiated retrieval of RUM reports, you have to log in to SSM On-Prem. Duplicate usernames may cause the feature to work incorrectly if there are present in the system.

Step 11	**username** *name* **privilege** *level* **password** *password*
	Example:
	`Device(config)# username admin privilege 15`
	`password 0 lab`
		(Required) Establishes a username-based authentication system.
		The **privilege** keyword sets the privilege level for the user. A number between 0 and 15 that specifies the privilege level for the user.
		The password allows access to the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
		This enables SSM On-Prem to use the product instance native REST.

	Command or Action	Purpose
		Note Enter this username and password in SSM On-Prem (Adding One or More Product Instances (SSM On-Prem UI), on page 138). This enables SSM On-Prem to collect RUM reports from the product instance.
Step 12	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 13	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 15	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 16	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts a disabled interface.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 18	**ip http server** **Example:** `Device(config)# ip http server`	(Required) Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. The HTTP server uses the standard port 80, by default.

Step 19	**ip http authentication local**
	Example:
	`ip http authentication local`
	`Device(config)#`
		(Required) Specifies a particular authentication method for HTTP server users.
		The **local** keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the username global

	Command or Action	Purpose
		configuration command) should be used for authentication and authorization.
Step 20	**ip http secure-server** **Example:** `Device(config)# ip http server`	(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.
Step 21	**ip http max-connections** **Example:** `Device(config)# ip http max-connections 16`	(Required) Configures the maximum number of concurrent connections allowed for the HTTP server. Enter an integer in the range from 1 to 16. The default is 5.
Step 22	**ip tftp source-interface** *interface-type-number* **Example:** `Device(config)# ip tftp source-interface GigabitEthernet0/0`	Specifies the IP address of an interface as the source address for TFTP connections.
Step 23	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 24	**logging host** **Example:** `Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	Logs system messages and debug output to a remote host.

Step 25	**crypto pki trustpoint SLA-TrustPoint**
	Example:
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		(Required) Declares that the product instance should use trustpoint "SLA-TrustPoint" and enters the ca-trustpoint configuration mode. The product instance does not recognize any trustpoints until you declare a trustpoint using this command.

Step 26	enrollment terminal **Example:** `Device(ca-trustpoint)# enrollment terminal`	Required) Specifies the certificate enrollment method.
Step 27	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	(Required) Specifies a method that is to be used to ensure that the certificate of a peer is not revoked. For the SSM On-Prem Deployment topology, enter the **none** keyword. This means that a revocation check will not be performed and the certificate will always be accepted.

	Command or Action	Purpose

Step 28	**end**
	Example:
	`Device(ca-trustpoint)# exit`
	`Device(config)# end`
		Exits the ca-trustpoint configuration mode and then the global configuration mode and returns to privileged EXEC mode.

Step 29	**show ip http server session-module** **Example:** `Device# show ip http server session-module`	(Required) Verifies HTTP connectivity. In the output, check that `SL_HTTP` is active. Additionally, you can also perform the following checks : • From device where SSM On-Prem is installed, verify that you can ping the product instance. A successful ping confirms that the product instance is reachable. • From a Web browser on the device where SSM On-Prem is installed verify `https://<product-instance-ip>/`. This ensures that the REST API from SSM On-Prem to the product instance works as expected.
Step 30	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Setting Up a Connection to CSSM

The following steps show how to set up a Layer 3 connection to CSSM to verify network reachability. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*]	Specifies the address of one or more name servers to use for name and address resolution.

	Command or Action	Purpose
	Example: `Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	**ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6* **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	(Optional) Configures DNS on the VRF interface. You can specify up to six name servers. Separate each server address with a space. **Note** This command is an alternative to the **ip name-server** command.
Step 5	**ip domain lookup source-interface** *interface-type interface-number* **Example:** `Device(config)# ip domain lookup source-interface Vlan100`	Configures the source interface for the DNS domain lookup.
Step 6	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configures the domain name.
Step 7	**ip host tools.cisco.com** *ip-address* **Example:** `Device(config)# ip host tools.cisco.com 209.165.201.30`	Configures static hostname-to-address mappings in the DNS hostname cache if automatic DNS mapping is not available.

Step 8	**interface** *interface-type-number*
	Example:
	`Device(config)# interface Vlan100`
	`Device(config-if)# ip address 192.0.2.10 255.255.255.0`
	`Device(config-if)# exit`
		Configures a Layer 3 interface. Enter an interface type and number or a VLAN.

Step 9	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Device(config)# ntp server 198.51.100.100 version 2 prefer`	(Required) Activates the NTP service (if it has not already been activated) and enables the system to synchronize the system software clock with the specified NTP server. This ensures that the device time is synchronized with CSSM. Use the **prefer** keyword if you need to use this command multiple times and you want to set a preferred server. Using this keyword reduces switching between servers.

	Command or Action	Purpose

Step 10	**switchport access vlan** *vlan_id*
	Example:
	`Device(config)# interface GigabitEthernet1/0/1`
	`Device(config-if)# switchport access vlan 100`
	`Device(config-if)# switchport mode access`
	`Device(config-if)# exit`
	`OR`
	`Device(config)#`
		Enables the VLAN for which this access port carries traffic and sets the interface as a nontrunking nontagged single-VLAN Ethernet interface.
		Note This step is to be configured only if the switchport access mode is required. The **switchport access vlan** command may apply to Catalyst switching product instances, for example, and for routing product instances you may want to configure the **ip address** *ip-address mask* command instead.

Step 11	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route 192.0.2.0 255.255.255.255 192.0.2.1`	Configures a route on the device. You can configure either a static route or a dynamic route.
Step 12	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface Vlan100`	(Required) Configures a source interface for the HTTP client. Enter an interface type and number or a VLAN.
Step 13	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 14	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Configuring Smart Transport Through an HTTPs Proxy

To use a proxy server to communicate with CSSM when using the Smart transport mode, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart transport smart** **Example:** `Device(config)# license smart transport smart`	Enables Smart transport mode.
Step 4	**license smart url default** **Example:** `Device(config)# license smart transport default`	Automatically configures the Smart URL (https://smartreceiver.cisco.com/licservice/license). For this option to work as expected, the transport mode in the previous step must be configured as **smart**.

Step 5	**license smart proxy** {**address** *address_hostname* | **port** *port_num*}
	Example:
	`Device(config)# license smart proxy address 192.168.0.1`
	`Device(config)# license smart proxy port 3128`
		Configures a proxy for the Smart transport mode. When a proxy is configured, licensing messages are sent to the proxy along with the final destination URL (CSSM). The proxy sends the message on to CSSM. Configure the proxy address and port number separately:
		• **address** *address_hostname*: Specifies the proxy address. Enter the IP address or hostname of the proxy server.
		• **port** *port_num*: Specifies the proxy port. Enter the proxy port number.
		Note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`. For more information about the status line, see section 3.1.2 of RFC 7230.

Configuring the Call Home Service for Direct Cloud Access

The Call Home service provides email-based and web-based notification of critical system events to CSSM. To configure the transport mode, enable the Call Home service, and configure a destination profile (A destination profile contains the required delivery information for an alert notification. At least one destination profile is required.), complete the following steps:

Note All steps are required unless specifically called-out as "(Optional)".

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart transport callhome** **Example:** `Device(config)# license smart transport callhome`	Enables Call Home as the transport mode.
Step 4	**license smart url** *url* **Example:** `Device(config)# license smart url https://tools.cisco.com/its/service/oddce/services/DDCEService`	For the **callhome** transport mode, configure the CSSM URL exactly as shown in the example.
Step 5	**service call-home** **Example:** `Device(config)# service call-home`	Enables the Call Home feature.
Step 6	**call-home** **Example:** `Device(config)# call-home`	Enters Call Home configuration mode.
Step 7	**no http secure server-identity-check** **Example:** `Device(config-call-home)# no http secure server-identity-check`	Disables server identity check when HTTP connection is established.
Step 8	**contact-email-address** *email-address* **Example:** `Device(config-call-home)# contact-email-addr username@example.com`	Assigns customer's email address and enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process. You can enter up to 200 characters in email address format with no spaces.

	Command or Action	Purpose

Step 9	**profile** *name*
	Example:
	`Device(config-call-home)# profile CiscoTAC-1`
	`Device(config-call-home-profile)#`
		Enters the Call Home destination profile configuration submode for the specified destination profile.
		By default:
		• The CiscoTAC-1 profile is inactive. To use this profile with the Call Home service, you must enable the profile.
		• The CiscoTAC-1 profile sends a full report of all types of events subscribed in the profile. The alternative is to additionally configure `Device(cfg-call-home-profile)# anonymous-reporting-only` anonymous-reporting-only. When this is set, only crash, inventory, and test messages will be sent.
		Use the **show call-home profile all** command to check the profile status.

Step 10	**active** **Example:** `Device(config-call-home-profile)# active`	Enables the destination profile.

Step 11	**destination transport-method http** {**email** |**http**}
	Example:
	`Device(config-call-home-profile)# destination transport-method http`
	`AND`
	`Device(config-call-home-profile)# no destination transport-method email`
		Enables the message transport method. In the example, Call Home service is enabled via HTTP and transport via email is disabled.
		The **no** form of the command disables the method.

Step 12	**destination address** { **email** *email_address* |**http** *url*}
	Example:
	`Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
	`AND`
	`Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
		Configures the destination e-mail address or URL to which Call Home messages are sent. When entering a destination URL, include either **http://** (default) or **https://**, depending on whether the server is a secure server.
		In the example provided here, a **http://** destination URL is configured; and the **no** form of the command is configured for **https://**.

	Command or Action	Purpose
Step 13	**exit** **Example:** `Device(config-call-home-profile)# exit`	Exits Call Home destination profile configuration mode and returns to Call Home configuration mode.
Step 14	**exit** **Example:** `Device(config-call-home)# end`	Exits Call Home configuration mode and returns to privileged EXEC mode.
Step 15	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.
Step 16	**show call-home profile** {*name* |**all**}	Displays the destination profile configuration for the specified profile or all configured profiles.

Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server

The Call Home service can be configured through an HTTPs proxy server. This configuration requires no user authentication to connect to CSSM.

Note Authenticated HTTPs proxy configurations are not supported.

To configure and enable the Call Home service through an HTTPs proxy, complete the following steps:

Note All steps are required unless specifically called-out as "(Optional)".

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**license smart transport callhome** **Example:** `Device(config)# license smart transport callhome`	Enables Call Home as the transport mode.
Step 4	**service call-home** **Example:** `Device(config)# service call-home`	Enables the Call Home feature.
Step 5	**call-home** **Example:** `Device(config)# call-home`	Enters Call Home configuration mode.
Step 6	**http-proxy** *proxy-address* **proxy-port** *port-number* **Example:** `Device(config-call-home)# http-proxy 198.51.100.10 port 5000`	Configures the proxy server information to the Call Home service. Note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`. For more information about the status line, see section 3.1.2 of RFC 7230.
Step 7	**exit** **Example:** `Device(config-call-home)# exit`	Exits Call Home configuration mode and enters global configuration mode.
Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 9	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Removing and Returning an Authorization Code

To remove and return an SLR authorization code, complete the following steps.

Before you begin

Supported topologies: all

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**show license summary** **Example:** `Device# show license summary`	Ensure that the license that you want to remove and return is not in-use. If it is in-use, you must first disable the feature.

Step 3	**license smart authorization return** {**all** | **local**} {**offline** [*path*] | **online**}
	Example:
	`Device# license smart authorization return all online`
	
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	`Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h`
	`UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA`
	
	`OR`
	
	`Device# license smart authorization return local offline`
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	`Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h`
	`UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA`
	
	`OR`
	
	`Device# license smart authorization return local offline bootflash:return-code.txt`
		Returns an authorization code back to the license pool in CSSM. A return code is displayed after you enter this command.
		Specify the product instance:
		• **all**: Performs the action for all connected product instances in a High Availability set-up.
		• **local**: Performs the action for the active product instance. This is the default option.
		Specify if you are connected to CSSM or not:
		• If connected to CSSM, enter **online**. The code is automatically returned to CSSM and a confirmation is returned and installed on the product instance. If you choose this option, the return code is automatically submitted to CSSM.
		• If not connected to CSSM, enter **offline**[*path*].
		If you enter only the **offline** keyword, you must copy the return code that is displayed on the CLI and enter it in CSSM.
		If you specify a file name and path, the return code is saved in the specified location. The file format can be any readable format. For example: `Device# license smart authorization return local offline bootflash:return-code.txt`.
		For software versions Cisco IOS XE Cupertino 17.7.1 and later only: After you save the return request in a file, you can upload the file to CSSM in the same location and in the same way as you upload a RUM report: #unique_161.

	Command or Action	Purpose
		To enter the return code in CSSM, complete this task: Removing the Product Instance from CSSM, on page 153. Proceed with the next step only after you complete this step.
Step 4	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 5	**no license smart reservation** **Example:** `Device(config)# no license smart reservation`	Disables SLR configuration on the product instance. You must complete the authorization code return process in Step 3 above - whether online or offline, before you enter the no license smart reservation command in this step. Otherwise, the return may not be reflected in CSSM or in the show command, and you will have to contact your Cisco technical support representative to rectify the problem.
Step 6	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Step 7	**show license all**
	Example:
	`Device# show license all`
	`<output truncated>`
	`License Authorizations`
	`======================`
	`Overall status:`
	`  Active: PID:C9800-CL-K9,SN:93BBAH93MGS`
	
	`  Status: NOT INSTALLED`
	`  Last return code:`
	`CopaUPW-WSPYiq-ZNU2ci-ShWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h`
	
	`  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN`
	
	`  Status: NOT INSTALLED`
	`  Last return code:`
	`CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA`
	`<output truncated>`
		Displays licensing information. Check the `License Authorizations` header in the output. If the return process is completed correctly, the `Last return code:` field displays the return code.

Removing the Product Instance from CSSM

To remove a product instance and return all licenses to the license pool, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

If you are removing a product instance that is using reserved licenses (SLR) ensure that you have generated a return code as shown in Removing and Returning an Authorization Code, on page 151. (Enter it in Step 7 in this task).

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**.

Log in using the username and password provided by Cisco.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose your Virtual Account.

Step 4 Click the **Product Instances** tab.

The list of product instances that are available is displayed.

Step 5 Locate the required product instance from the product instances list. Optionally, you can enter a name or product type string in the search tab to locate the product instance.

Step 6 In the **Actions** column of the product instance you want to remove, click the **Remove** link.

- If the product instance is *not* using a license with an SLR authorization code then the **Confirm Remove Product Instance** window is displayed.
- If the product instance *is* using a license with an SLR authorization code, then the **Remove Product Instance** window, with a field for return code entry is displayed.

Step 7 In the **Reservation Return Code** field, enter the return code you generated.

Note This step applies only if the product instance is using a license with an SLR authorization code.

Step 8 Click **Remove Product Instance**.

The license is returned to the license pool and the product instance is removed.

Generating a New Token for a Trust Code from CSSM

To generate a token to request a trust code, complete the following steps.

Generate one token for each *Virtual Account* you have. You can use same token for all the product instances that are part of one Virtual Account.

Before you begin

Supported topologies: Connected Directly to CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**.

Log in using the username and password provided by Cisco.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose the required virtual account

Step 4 Click the **General** tab.

Step 5 Click **New Token**. The **Create Registration Token** window is displayed.

Step 6 In the **Description** field, enter the token description

Step 7 In the **Expire After** field, enter the number of days the token must be active.

Step 8 (Optional) **In the Max. Number of Uses** field, enter the maximum number of uses allowed after which the token expires.

Step 9 Click **Create Token**.

Note If you enter a value here, ensure that you stagger the installation of the trust code on the product instances, which is the next part of the process. If you want to simultaneously install the trust code on a large number of product instances, we recommend that you leave this field blank. Entering a limit here and simultaneously installing it on a large number of devices causes a bottleneck in the processing of these requests in CSSM and installation on some devices may fail, with the following error: `Failure Reason: Server error occurred: LS_LICENGINE_FAIL_TO_CONNECT.`

Step 10 You will see your new token in the list. Click **Actions** and download the token as a `.txt` file.

Installing a Trust Code

To manually install a trust code, complete the following steps

Before you begin

Supported topologies:

- Connected Directly to CSSM

Procedure

	Command or Action	Purpose
Step 1	#unique_157	In case you have not completed this already, generate and download a trust code file from CSSM.
Step 2	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted

	Command or Action	Purpose
Step 3	**license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] **Example:** `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	Enables you to establish a trusted connection with CSSM. For *id_token_value*, enter the token you generated in CSSM. Enter one of following options: • **local**: Submits the trust request only for the active device in a High Availability set-up. This is the default option. • **all**: Submits the trust request for all devices in a High Availability set-up. Enter the **force** keyword to submit the trust code request in spite of an existing trust code on the product instance. Trust codes are node-locked to the UDI of the product instance. If a UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one already exists.

Step 4	**show license status**
	Example:
	`<output truncated>`
	`Trust Code Installed:`
	`  Active: PID:C9800-CL-K9,SN:93BBAH93MGS`
	`    INSTALLED on Nov 02 08:59:26 2020 IST`
	`  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`    INSTALLED on Nov 02 09:00:45 2020 IST`
		Displays date and time if trust code is installed. Date and time are in the local time zone. See field `Trust Code Installed:`.

Downloading a Policy File from CSSM

If you have requested a custom policy or if you want to apply a policy that is different from the default that is applied to the product instance, complete the following task:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**.

Log in using the username and password provided by Cisco.

Step 2 Follow this directory path: **Reports** > **Reporting Policy**.

Step 3 Click **Download**, to save the `.xml` policy file.

You can now install the file on the product instance. See #unique_164

Uploading Data or Requests to CSSM and Downloading a File

You can use this task to:

- To upload a RUM report to CSSM and download an ACK.
- To upload a SLAC or SLR authorization code return request.

  This applies only to the *No Connectivity to CSSM and No CSLU* topology and is supported starting with Cisco IOS XE Cupertino 17.7.1.

To upload a RUM report to CSSM and download an ACK *when the product instance is not connected to CSSM or CSLU*, complete the following task:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM
- SSM On-Prem Deployment (Product instance-initiated communication and SSM On-Prem-initiated communication)

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com.

Log in using the username and password provided by Cisco.

Step 2 Select the **Smart Account** (upper left-hand corner of the screen) that will receive the report.

Step 3 Select **Smart Software Licensing** → **Reports** → **Usage Data Files**.

Step 4 Click **Upload Usage Data**. Browse to the file location (RUM report in tar format), select, and click **Upload Data**.

Upload a RUM report (`.tar` format), or a SLAC return request file (`.txt` format).

You cannot delete a usage report in CSSM, after it has been uploaded.

Step 5 From the Select Virtual Accounts pop-up, select the **Virtual Account** that will receive the uploaded file. The file is uploaded to Cisco and is listed in the Usage Data Files table in the Reports screen showing the File Name, time is was Reported, which Virtual Account it was uploaded to, the Reporting Status, Number of Product Instances reported, and the Acknowledgement status.

Step 6 In the Acknowledgement column, click **Download** to save the `.txt` ACK file for the report you uploaded.

Wait for the ACK to appear in the Acknowledgement column. If there many RUM reports or requests to process, CSSM may take a few minutes.

Depending on the topology you have implemented, you can now install the file on the product instance, or transfer it to CSLU, or import it into SSM On-Prem.

Installing a File on the Product Instance

To install a SLAC, or policy, or ACK, on the product instance *when the product instance is not connected to CSSM or CSLU*, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

You must have the corresponding file saved in a location that is accessible to the product instance.

- For a policy, see #unique_205
- For an ACK, see #unique_161

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted
Step 2	**copy** *source* **bootflash:***file-name* **Example:** `Device# copy tftp://10.8.0.6/example.txt bootflash:`	Copies the file from its source location or directory to the flash memory of the product instance. • *source*: This is the location of the source file or directory to be copied. The source can be either local or remote • **bootflash:**: This is the destination for boot flash memory.
Step 3	**license smart import bootflash:** *file-name* **Example:** `Device# license smart import bootflash:example.txt`	Imports and installs the file on the product instance. After installation, a system message displays the type of file you just installed.

	Command or Action	Purpose
Step 4	**show license all** **Example:** `Device# show license all`	Displays license authorization, policy and reporting information for the product instance.

Setting the Transport Type, URL, and Reporting Interval

To configure the mode of transport for a product instance, complete the following task:

Before you begin

Supported topologies: all

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	
Step 3	**license smart transport** {**automatic** | **callhome** | **cslu** | **off** | **smart**} **Example:** `Device(config)# license smart transport cslu`	Configures a mode of transport for the product instance to use. Choose from the following options: • **automatic**: Sets the transport mode **cslu**. • **callhome**: Enables Call Home as the transport mode. • **cslu**: This is the default transport mode. Enter this keyword if you are using CSLU *or* SSM On-Prem, with product instance-initiated communication. While the transport mode keyword is the same for CSLU and SSM On-Prem, the transport URLs are different. See **license smart url cslu** *cslu_or_on-prem_url* in the next step. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport.

	Command or Action	Purpose

Step 4	**license smart url** {*url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *smart_url*}
	Example:
	`Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi`
		Sets a URL for the configured transport mode. Depending on the transport mode you've chosen in the previous step, configure the corresponding URL here:
		• *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:
		`https://tools.cisco.com/its/service/oddce/services/DDCEService`
		The **no license smart url***url* command reverts to the default URL.
		• **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option with the URL for CSLU or SSM On-Prem, as applicable.
		  • If you are using CSLU, enter the URL as follows:
		  `http://<cslu_ip_or_host>:8182/cslu/v1/pi`
		  For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.
		  The **no license smart url cslu** *cslu_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`
		  • If you are using SSM On-Prem, enter the URL as follows:
		  `http://<ip>/cslu/v1/pi/<tenant ID>`
		  For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.
		  Tip You can retrieve the entire URL from SSM On-Prem. See Retrieving the Transport URL (SSM On-Prem UI), on page 137

	Command or Action	Purpose
		The **no license smart url cslu** *cslu_url* command reverts to `http://cslu-local:8182/cslu/v1/pi` • **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option. If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically (`https://cslu-local:8182/cslu/v1/pi`). If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`). • **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows: `https://smartreceiver.cisco.com/licservice/license` When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required. The **no license smart url smart***smart_url* command reverts to the default URL. • **utility** *smart_url*: Although available on the CLI, this option is not supported.
Step 5	**license smart usage interval** *interval_in_days* **Example:** `Device(config)# license smart usage interval 40`	(Optional) Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650. If you do not configure an interval, the reporting interval is determined entirely by the policy value.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:**	Saves your entries in the configuration file.

	Command or Action	Purpose
	`Device# copy running-config startup-config`	

Configuring an AIR License

In the Smart Licensing Using Policy environment, you can use this task to configure a license, or change the license being used on the product instance, or configure an add-on license on the product instance. For example, if you are currently using AIR Network Advantage and you also want to use features available with a corresponding Digital Networking Architecture (DNA) Advantage license, you can configure the same using this task. Or for example, if you do not want to use an add-on license any more, reconfigure this command to use only the AIR Network Advantage license.

Information about available licenses can be found Smart Account or Virtual Account. The available licenses may be one of the following:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

To configure or change the license in-use, follow this procedure:

Before you begin

Supported topologies: all

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 3	**license air level** {**air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] } **Example:** `Device(config)# license air level air-network-essentials addon air-dna-essentials`	Activates the configured license on the product instance. In the accompanying example, the product instance activates the AIR DNA Essentials (along with the AIR Network Essential) license after reload.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to the privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves configuration changes.
Step 6	**reload** **Example:** `Device# reload`	Reloads the device.

Step 7	**show version**
	Example:
	`Device# show version`
	`Cisco IOS XE Software, Version 17.03.02`
	`Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2, RELEASE SOFTWARE`
	`<output truncated>`
	`AIR License Level: AIR DNA Essentials`
	`Next reload AIR license Level: AIR DNA Essentials`
	
	`Smart Licensing Status: Registration Not Applicable/Not Applicable`
	`<output truncated>`
		Displays currently used license and the license that is effective at the next reload information.

What to do next

After you configure a license level, the change is effective after a reload. To know if reporting is required, refer to the output of the **show license status** privileged EXEC command and check the `Next ACK deadline:` and `Next report push:` fields.

Note The change in license usage is recorded on the product instance. The next steps relating to reporting - if required - depend on your current topology.

- Connected to CSSM Through CSLU
  - Product Instance-initiated communication: The product instance triggers reporting and installs the returning ACK. CSLU sends the RUM report to CSSM and collects the ACK from CSSM.
  - CSLU-initiated communication: You have to collect usage from the CSLU interface: #unique_151. CSLU sends the RUM report to CSSM and collects the ACK from CSSM.
- Connected Directly to CSSM: The product instance triggers reporting and installs the returning ACK.
- CSLU Disconnected from CSSM:

- Product Instance-initiated communication: The product instance triggers reporting. You then have to report usage in the disconnected mode: #unique_160 > #unique_161 > #unique_162.
- CSLU-initiated communication: You have to collect usage from the CSLU interface and report usage in the disconnected mode: #unique_151> #unique_160 > #unique_161 > #unique_162.

- No Connectivity to CSSM and No CSLU: License usage is recorded on the product instance. You must save RUM reports to a file on the product instance, and from a workstation that has connectivity to the internet, and Cisco, upload it to CSSM: Enter **license smart save usage** privileged EXEC command to save usage > #unique_161 > #unique_164.

Sample Resource Utilization Measurement Report

The following is a sample Resource Utilization Measurement (RUM) report, in XML format (See #unique_107). Several such reports may be concatenated to form one report.

```
<?xml version="1.0" encoding="UTF-8"?>
  <smartLicense>
```

```
  </smartLicense>
```

Troubleshooting Smart Licensing Using Policy

This section provides the list of Smart Licensing Using Policy-related system messages you may encounter, possible reasons for failure, and recommended action.

System Message Overview

The system software sends system messages to the console (and, optionally, to a logging server on another system). Not all system messages mean problems with your system. Some messages are informational, and others can help diagnose problems with communications lines, internal hardware, or the system software.

How to Read System Messages

System log messages can contain up to 80 characters. Each system message begins with a percent sign (%) and is structured as follows:

```
%FACILITY-SEVERITY-MNEMONIC: Message-text
```

%FACILITY

Two or more uppercase letters that show the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software

SEVERITY

A single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.

Table 11: Message Severity Levels

Severity Level	Description
0 - emergency	System is unusable.
1 - alert	Immediate action required.
2 - critical	Critical condition.
3 - error	Error condition.
4 - warning	Warning condition.
5 - notification	Normal but significant condition.
6 - informational	Informational message only.
7 - debugging	Message that appears during debugging only.

MNEMONIC

A code that uniquely identifies the message.

Message-text

Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec].

Table 12: Variable Fields in Messages

Severity Level	Description
[char]	Single character
[chars]	Character string
[dec]	Decimal number
[enet]	Ethernet address (for example, 0000.FEED.00C0)
[hex]	Hexadecimal number
[inet]	Internet address (for example, 10.0.2.16)
[int]	Integer
[node]	Address or node name
[t-line]	Terminal line number in octal (or in decimal if the decimal-TTY service is enabled)
[clock]	Clock (for example, 01:20:08 UTC Tue Mar 2 1993

System Messages

This section provides the list of Smart Licensing Using Policy-related system messages you may encounter, possible reasons for failure (incase it is a failure message), and recommended action (if action is required).

For all error messages, if you are not able to solve the problem, contact your Cisco technical support representative with the following information:

The message, exactly as it appears on the console or in the system log.

The output from the **show license tech support**, **show license history message**, and the **show platform software sl-infra** privileged EXEC commands.

- %SMART_LIC-3-POLICY_INSTALL_FAILED
- %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED
- %SMART_LIC-3-COMM_FAILED
- %SMART_LIC-3-COMM_RESTORED
- %SMART_LIC-3-POLICY_REMOVED
- %SMART_LIC-3-TRUST_CODE_INSTALL_FAILED
- %SMART_LIC-4-REPORTING_NOT_SUPPORTED
- %SMART_LIC-6-POLICY_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_REMOVED
- %SMART_LIC-6-REPORTING_REQUIRED
- %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS
- %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG
- %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED

```
Error Message %SMART_LIC-3-POLICY_INSTALL_FAILED: The installation of a new
licensing policy has failed: [chars].
```

Explanation: A policy was installed, but an error was detected while parsing the policy code, and installation failed. [chars] is the error string with details of the failure.

Possible reasons for failure include:

- A signature mismatch: This means that the system clock is not accurate.
- A timestamp mismatch: This means the system clock on the product instance is not synchronized with CSSM.

Note The device should have a valid clock and the NTP configuration.

Recommended Action:

For both possible failure reasons, ensure that the system clock is accurate and synchronized with CSSM. Configure the **ntp server** command in global configuration mode. For example:

```
Device(config)# ntp server 198.51.100.100 version 2 prefer
```

If the above does not work and policy installation still fails, and contact your Cisco technical support representative.

```
Error Message %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED: The install of a new
licensing authorization code has failed on [chars]: [chars].
```

This message is not applicable to Cisco Catalyst Access, Core, and Aggregation Switches, because there are no enforced or export-controlled licenses on these product instances.

```
Error Message %SMART_LIC-3-COMM_FAILED: Communications failure with the [chars] :
[chars]
```

Explanation: Smart Licensing communication either with CSSM, or CSLU, or SSM On-Prem failed. The first [chars] is the currently configured transport type, and the second [chars] is the error string with details of the failure. This message appears for every communication attempt that fails.

Possible reasons for failure include:

- CSSM, CSLU, SSM On-Prem is not reachable: This means that there is a network reachability problem.
- 404 host not found: This means the CSSM server is down.
- A TLS or SSL handshake failure caused by a missing client certificate. The certificate is required for TLS authentication of the two communicating sides. A recent server upgrade may have cause the certificate to be removed. This reason applies only to a topology where the product instance is directly connected to CSSM.

Note If the error message is displayed for this reason, there is no actual configuration error or disruption in the communication with CSSM.

For topologies where the product instance initiates the sending of RUM reports (Connected to CSSM Through CSLU: Product Instance-Initiated Communication, Connected Directly to CSSM, CSLU Disconnected from CSSM: Product Instance-Initiated Communication, and SSM On-Prem Deployment: Product Instance-Initiated Communication) if this communication failure message coincides with scheduled reporting (**license smart usage interval** *interval_in_days* global configuration command), the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to last configured value.

Recommended Action:

Troubleshooting steps are provided for when CSSM is not reachable or there is a missing client certificate, when CSLU is not reachable, and when SSM On-Prem is not reachable.

- If a client certificate is missing and there is no actual configuration error or disruption in the communication with CSSM:

  To resolve the error, configure the **ip http client secure-trustpoint** *trustpoint-name* command in global configuration mode. For *trustpoint-name*, enter only `SLA-TrustPoint`. This command specifies that the secure HTTP client should use the certificate associated with the trustpoint indicated by the trustpoint-name argument.

- If CSSM is not reachable and the configured transport type is **smart**:

  1. Check if the smart URL is configured correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://smartreceiver.cisco.com/licservice/license. If it is not, reconfigure the **license smart url smart** *smar_URL* command in global configuration mode.
  2. Check DNS resolution. Verify that the product instance can ping `smartreceiver.cisco.com` or the nslookup translated IP. The following example shows how to ping the translated IP

     ```
     Device# ping 171.70.168.183
     Type escape sequence to abort.
     Sending 5, 100-byte ICMP Echos to 171.70.168.183, timeout is 2 seconds:
     !!!!!
     Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
     ```

- If CSSM is not reachable and the configured transport type is **callhome**:

  1. Check if the URL is entered correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://tools.cisco.com/its/service/oddce/services/DDCEService.
  2. Check if Call Home profile `CiscoTAC-1` is active and destination URL is correct. Use the **show call-home profile all** command in privileged EXEC mode:

     ```
     Current smart-licensing transport settings:
      Smart-license messages: enabled
      Profile: CiscoTAC-1 (status: ACTIVE)
      Destination  URL(s):  https://tools.cisco.com/its/service/oddce/services/DDCEService
     ```

  3. Check DNS Resolution. Verify that the product instance can ping `tools.cisco.com`, or the nslookup translated IP.

     ```
     Device# ping tools.cisco.com
     Type escape sequence to abort.
     Sending 5, 100-byte ICMP Echos to 173.37.145.8, timeout is 2 seconds:
     !!!!!
     Success rate is 100 percent (5/5), round-trip min/avg/max = 41/41/42 ms
     ```

     If the above does not work check the following: if the product instance is set, if the product instance IP network is up. To ensure that the network is up, configure the **no shutdown** command in interface configuration mode.

     Check if the device is subnet masked with a subnet IP, and if the DNS IP is configured.

  4. Verify that the HTTPs client source interface is correct.

     Use the **show ip http client** command in privileged EXEC mode to display current configuration. Use **ip http client source-interface** command in global configuration mode to reconfigure it.

     In case the above does not work, double-check your routing rules, and firewall settings.

- If CSLU is not reachable:

  1. Check if CSLU discovery works.

     - Zero-touch DNS discovery of `cslu-local` or DNS discovery of your domain..

       In the **show license all** command output, check if the `Last ACK received:` field. If this has a recent timestamp it means that the product instance has connectivity with CSLU. If it is not, proceed with the following checks:

       Check if the product instance is able to ping `cslu-local`. A successful ping confirms that the product instance is reachable.

       If the above does not work, configure the name server with an entry where hostname `cslu-local` is mapped to the CSLU IP address (the windows host where you installed CSLU). Configure the **ip domain name** *domain-name* and **ip name-server** *server-address* commands in global configuration mode. Here the CSLU IP is 192.168.0.1 and name-server creates entry `cslu-local.example.com`:

       ```
       Device(config)# ip domain name example.com
       Device(config)# ip name-server 192.168.0.1
       ```

     - CSLU URL is configured.

       In the **show license all** command output, under the `Transport:` header check the following: The `Type:` must be `cslu`and `Cslu address:` must have the hostname or the IP address of the windows host where you have installed CSLU. Check if the rest of the address is configured as shown below and check if the port number is 8182.

       ```
       Transport:
         Type: cslu
         Cslu address: http://192.168.0.1:8182/cslu/v1/pi
       ```

       If it is not, configure the **license smart transport cslu** and **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* commands in global configuration mode

  2. For CSLU-initiated communication, in addition to the CSLU discovery checks listed above, check the following:

     Verify HTTP connectivity. Use the **show ip http server session-module** command in privileged EXEC mode. In the output, under header `HTTP server current connections:`, check that `SL_HTTP` is active. If it is not re-configure the **ip http** commands as mentioned in #unique_150

     From a Web browser on the device where CSLU is installed, verify `https://<product-instance-ip>/`. This ensures that the REST API from CSLU to the product instance works as expected.

- If SSM On-Prem is not reachable:

  1. For product instance-initiated communication, check if the SSM On-Prem transport type and URL are configured correctly.

     In the **show license all** command output, under the `Transport:` header check the following: The `Type:` must be `cslu`and `Cslu address:` must have the hostname or the IP address of the server where you have installed SSM On-Prem and <tenantID> of the *default* local virtual account. See the example below:

     ```
     Transport:
       Type: cslu
       Cslu address: https://192.168.0.1/cslu/v1/pi/on-prem-default
     ```

Check if you have the correct URL from SSM On-Prem (Retrieving the Transport URL (SSM On-Prem UI), on page 137) and then configure **license smart transport cslu** and **license smart url cslu** *http://<ip>/cslu/v1/pi/<tenant ID>* commands in global configuration mode.

Check that you have configured any other required commands for your network as mentioned in Ensuring Network Reachability for Product Instance-Initiated Communication, on page 134.

2. For SSM On-Prem-initiated communication, check HTTPs connectivity.

   Use the **show ip http server session-module** command in privileged EXEC mode. In the output, under header `HTTP server current connections:`, check that `SL_HTTP` is active. If it is not re-configure the **ip http** commands as mentioned in Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 139.

3. Check trustpoint and that certificates are accepted.

   For both forms of communication in an SSM On-Prem Deployment, ensure that the correct trustpoint is used and that the necessary certificates are accepted:

```
Device(config)# crypto pki trustpoint SLA-TrustPoint
Device(ca-trustpoint)#
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device# copy running-config startup-config
```

If the above does not work and policy installation still fails, contact your Cisco technical support representative.


```
Error Message  %SMART_LIC-3-COMM_RESTORED: Communications with the [chars] restored.
[chars] - depends on the transport type
        - Cisco Smart Software Manager (CSSM)
        - Cisco Smart License utility (CSLU)
Smart Agent communication with either the Cisco Smart Software Manager (CSSM) or the Cisco
 Smart License
utility (CSLU) has been restored. No action required.
```

Explanation: Product instance communication with either the CSSM, or CSLU, or SSM On-Prem is restored.

Recommended Action: No action required.


```
Error Message %SMART_LIC-3-POLICY_REMOVED: The licensing policy has been removed.
```

Explanation: A previously installed *custom* licensing policy has been removed. The `Cisco default` policy is then automatically effective. This may cause a change in the behavior of smart licensing.

Possible reasons for failure include:

If you have entered the **license smart factory reset** command in privileged EXEC mode all licensing information including the policy is removed.

Recommended Action:

If the policy was removed intentionally, then no further action is required.

If the policy was removed inadvertantly, you can reapply the policy. Depending on the topology you have implemented, follow the corresponding method to retrieve the policy:

- Connected Directly to CSSM:

  Enter **show license status**, and check field `Trust Code Installed:`. If trust is established, then CSSM will automatically return the policy again. The policy is automatically re-installed on product instances of the corresponding Virtual Account.

  If trust has not been established, complete these tasks: #unique_157 and #unique_158. When you have completed these tasks, CSSM will automatically return the policy again. The policy is then automatically installed on all product instances of that Virtual Account.

- Connected to CSSM Through CSLU:

  - For product instance-initiated communication), enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the product instance.
  - For CSLU-initiated communication, complete this task: #unique_151. This causes CSLU to detect and re-furnish the missing policy in an ACK response.

- CSLU Disconnected from CSSM:

  - For product instance-initiated communication), enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the product instance. Then complete these tasks in the given order:#unique_160 > Uploading Data or Requests to CSSM and Downloading a File, on page 157 > #unique_162.
  - For CSLU-initiated communication, complete this task: #unique_151. This causes CSLU to detect and re-furnish the missing policy in an ACK response. Then complete these tasks in the given order: #unique_160 > Uploading Data or Requests to CSSM and Downloading a File, on page 157 > #unique_162.

- No Connectivity to CSSM and No CSLU

  If you are in an entirely air-gapped network, from a workstation that has connectivity to the internet and CSSM complete this task: #unique_205.

  Then complete this task on the product instance: #unique_164.

- SSM On-Prem Deployment

  - For product instance-initiated communication), enter the **license smart sync** command in privileged EXEC mode. The causes the product instance to synchronize with SSM On-Prem and restore any required or missing information. Then synchronize SSM On-Prem with CSSM if required:
  - For SSM On-Prem-initiated communication: In the SSM On-Prem UI, navigate to **Reports** > **Synchronization pull schedule with the devices** > **Synchronize now with the device**.

  For both forms of communication in an SSM On-Prem Deployment, synchronize with CSSM using either option:

  - SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
  - SSM On-Prem is not connected to CSSM: Exporting and Importing Usage Data (SSM On-Prem UI), on page 137.

```
Error Message %SMART_LIC-3-TRUST_CODE_INSTALL_FAILED: The install of a new licensing
trust code has failed on [chars]: [chars].
```

Explanation: Trust code installation has failed. The first [chars] is the UDI where trust code installation was attempted. The second [chars] is the error string with details of the failure.

Possible reasons for failure include:

- A trust code is already installed: Trust codes are node-locked to the UDI of the product instance. If the UDI is already registered, and you try to install another one, installation fails.
- Smart Account-Virtual Account mismatch: This means the Smart Account or Virtual Account (for which the token ID was generated) does not include the product instance on which you installed the trust code. The token generated in CSSM, applies at the Smart Account or Virtual Account level and applies only to all product instances in that account.
- A signature mismatch: This means that the system clock is not accurate.
- Timestamp mismatch: This means the product instance time is not synchronized with CSSM, and can cause installation to fail.

Recommended Action:

- A trust code is already installed: If you want to install a trust code inspite of an existing trust code on the product instance, re-configure the **license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] command in privileged EXEC mode, and be sure to include the **force** keyword this time. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one already exists.
- Smart Account-Virtual Account mismatch:

  Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**>**Inventory** > **Product Instances**.

  Check if the product instance on which you want to generate the token is listed in the selected Virtual Account. If it is, proceed to the next step. If not, check and select the correct Smart Account and Virtual Account. Then complete these tasks again: #unique_157 and #unique_158.
- Timestamp mismatch and signature mismatch: Configure the **ntp server** command in global configuration mode. For example:

  ```
  Device(config)# ntp server 198.51.100.100 version 2 prefer
  ```

```
Error Message    %SMART_LIC-4-REPORTING_NOT_SUPPORTED: The CSSM OnPrem that this
product instance is connected to is down rev and does not support the enhanced policy and
usage
reporting mode.
```

Explanation: Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) is supported in the Smart Licensing Using Policy environment starting with Cisco IOS XE Amsterdam

17.3.3 only (See SSM On-Prem, on page 63). In *unsupported* releases, the product instance will behave as follows:

- Stop sending registration renewals and authorization renewals.
- Start recording usage and saving RUM reports locally.

Recommended Action:

You have the following options:

- Refer to and implement one of the supported topologies instead. See: #unique_96.
- Upgrade to a release where SSM On-Prem is supported with Smart Licensing Using Policy. See Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 119.

```
Error Message %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed.
```

Explanation: A policy was installed in one of the following ways:

- Using Cisco IOS commands.
- CSLU-initiated communication.
- As part of an ACK response.

Recommended Action: No action is required. If you want to know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command in privileged EXEC mode.

```
Error Message %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was successfully installed on: [chars].
```

This message is not applicable to Cisco Catalyst Access, Core, and Aggregation Switches, because there are no enforced or export-controlled licenses on these product instances.

```
Error Message %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has
 been removed from [chars]
```

Explanation: [chars] is the UDI where the authorization code was installed. The authorization code has been removed. This removes the licenses from the product instance and may cause a change in the behavior of smart licensing and the features using licenses.

Recommended Action: No action is required. If you want to see the current state of the license, enter the **show license all** command in privileged EXEC mode.

```
Error Message %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in [dec] days.
```

Explanation: This is an alert which means that RUM reporting to Cisco is required. [dec] is the amount of time (in days) left to meet this reporting requirements.

Recommended Action: Ensure that RUM reports are sent within the requested time. The topology you have implemented determines the reporting method.

- Connected to CSSM Through CSLU
  - For product instance-initiated communication: Enter the **license smart sync** command in privileged EXEC mode. If CSLU is currently logged into CSSM the reports will be automatically sent to the associated Smart Account and Virtual Account in CSSM.
  - For CSLU-initiated communication, complete this task: #unique_151.
- Connected Directly to CSSM: Enter the **license smart sync** command in privileged EXEC mode.
- Connected to CSSM Through a Controller: If the product instance is managed by a controller, the controller will send the RUM report at the scheduled time.

  If you are using Cisco Catalyst Center as the controller, you have the option of ad-hoc reporting. See the *Cisco Catalyst Center Administrator Guide* of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Upload Resource Utilization Details to CSSM*.
- CSLU Disconnected from CSSM: If the product instance is connected to CSLU, synchronize with the product instance as shown for "Connected to CSSM Through CSLU"above, then complete these tasks: #unique_160, #unique_161, and #unique_162.
- No Connectivity to CSSM and No CSLU: Enter the **license smart save usage** command in privileged EXEC mode, to save the required usage information in a file. Then, from a workstation where you have connectivity to CSSM, complete these tasks: #unique_161 > #unique_164.
- SSM On-Prem Deployment:

  Synchronize the product instance with SSM On-Prem:
  - For product instance-initiated communication: Enter the **license smart sync** command in privileged EXEC mode. If CSLU is currently logged into CSSM the reports will be automatically sent to the associated Smart Account and Virtual Account in CSSM.
  - For SSM On-Prem-initiated communication, complete this task: In the SSM On-Prem UI, navigate to **Reports** > **Synchronization pull schedule with the devices** > **Synchronize now with the device**.

  Synchronize usage information with CSSM (*choose one*)
  - SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
  - SSM On-Prem is not connected to CSSM: Exporting and Importing Usage Data (SSM On-Prem UI), on page 137.

```
Error Message %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS: A new licensing trust code
 was successfully installed on [chars].
```

Explanation:[chars] is the UDI where the trust code was successfully installed.

Recommended Action: No action is required. If you want to verify that the trust code is installed, enter the **show license status** command in privileged EXEC mode. Look for the updated timestamp under header `Trust Code Installed:` in the output.


```
Error Message %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG: Unregistered 9800-CL can only
be used in lab. For production usage, please register this device in [int] days. Failure
to do so
will result in a limited number [50] of Access Points being allowed post this.
```

Explanation: An ACK is required on this product instance. [int] is the amount of time left to install an ACK on the product instance.

This is system message is displayed only if the product instance is a Cisco Catalyst 9800-CL Wireless Controller running Cisco IOS XE Cupertino 17.7.1 or a later release. For more information, see RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121 .

This system message is displayed once everyday, until the first ACK is made available on the product instance.

Recommended Action:

Implement one of the supported topologies and complete usage reporting. The method you can use to send the RUM report to CSSM and ACK installation depends on the topology you implement. See: Supported Topologies, on page 69 and How to Configure Smart Licensing Using Policy: Workflows by Topology , on page 86.


```
Error Message %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED: Chassis 1 R0/0:
wncmgrd: Ap MAC: [enet] is not allowed to join. Please start reporting licensing to Cisco
to get the
 ACK for resumption of usual operation.
```

Explanation: The ACK deadline for this product instance has passed and an ACK has still not been installed. [enet] is the MAC address of the AP that is trying to join the Cisco Catalyst 9800-CL Wireless Controller but is not allowed because the requisite ACK is not installed.

This is system message is displayed only if the product instance is a Cisco Catalyst 9800-CL Wireless Controller running Cisco IOS XE Cupertino 17.7.1 or a later release. For more information, see RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121 .

Recommended Action:

Implement one of the supported topologies and complete usage reporting. The method you can use to send the RUM report to CSSM and ACK installation depends on the topology you implement. See: Supported Topologies, on page 69 and How to Configure Smart Licensing Using Policy: Workflows by Topology , on page 86.

Additional References for Smart Licensing Using Policy

Topic	Document Title
For complete syntax and usage information for the commands used in this chapter, see the Command Reference of the corresponding release.	Cisco Catalyst 9800 Series Wireless Controller Command Reference
Cisco Smart Software Manager Help	Smart Software Manager Help
Cisco Smart License Utility (CSLU) installation and user guides	Cisco Smart License Utility Quick Start Setup Guide Cisco Smart License Utility User Guide

Feature History for Smart Licensing Using Policy

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

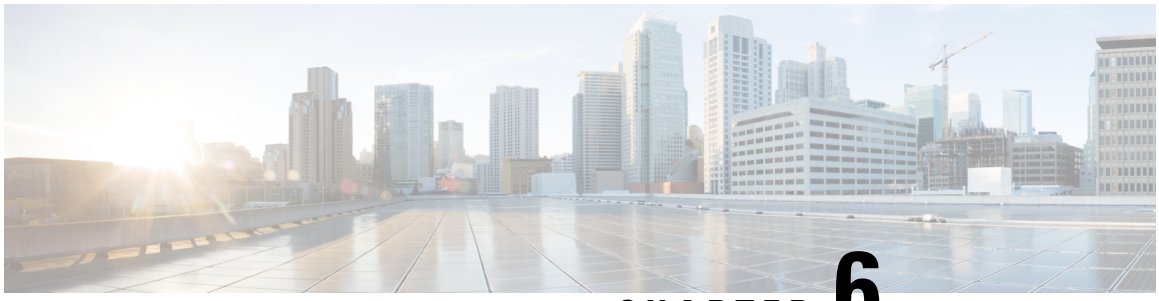
Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.10.1	Smart Licensing	A cloud-based, software license management solution that allows you to manage and track the status of your license, hardware, and software usage trends.

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.3.2a	Smart Licensing Using Policy	An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy.
	Cisco Catalyst Center Support for Smart Licensing Using Policy	Cisco Catalyst Center supports Smart Licensing Using Policy functionality starting with Cisco Catalyst Center Release 2.2.2. When you use Cisco Catalyst Center to manage a product instance, Cisco Catalyst Center connects to CSSM, and is the interface for all communication to and from CSSM. For information about the compatible controller and product instance versions, see Controller, on page 62. For information about this topology, see Connected to CSSM Through a Controller, on page 74 and Workflow for Topology: Connected to CSSM Through a Controller, on page 93.
Cisco IOS XE Amsterdam 17.3.3	Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM. For information about the compatible SSM On-Prem and product instance versions, see: SSM On-Prem, on page 63. For an overview of this topology, and to know how to implement it see SSM On-Prem Deployment, on page 77 and Workflow for Topology: SSM On-Prem Deployment, on page 95. For information about migrating from an existing version of SSM On-Prem, to one that supports Smart Licensing Using Policy, see Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 119.

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.7.1	RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller	If you are using a Cisco Catalyst 9800-CL Wireless Controller, you must complete RUM reporting and ensure that the Acknowledgment (ACK) is made available on the product instance - at least once. This is to ensure that correct and up-to-date usage information is reflected in CSSM. For more information, see RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 121.
	Factory-installed trust code	For new hardware orders, a trust code is now installed at the time of manufacturing. Note: You cannot use a factory-installed trust code to communicate with CSSM. See: Overview, on page 60 and Trust Code, on page 68.
	Support for trust code in additional topologies	A trust code is automatically obtained in topologies where the product instance initiates the sending of data to *CSLU* and in topologies where the product instance is in an air-gapped network. See: • Trust Code, on page 68 • Connected to CSSM Through CSLU, on page 69, #unique_117 unique_117_Connect_42_section_d3n_5dq_1nb. • CSLU Disconnected from CSSM, on page 73, #unique_120 unique_120_Connect_42_section_gb1_jdr_1nb. • No Connectivity to CSSM and No CSLU, on page 75, Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 94.
	RUM Report optimization and availability of statistics	

Release	Feature	Feature Information
		RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). See RUM Report and Report Acknowledgement, on page 67. Also see the **show license rum**, **show license all**, and **show license tech** commands in the command reference of the applicable release.
	Support to collect software version in a RUM report	If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and Smart Agent version information is *included* in the RUM report. See the **license smart** global configuration command in the command reference of the applicable release.
	Account information included in the ACK and **show** command outputs	A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. You can then display account information using various **show** commands. The account information that is displayed is always as per the latest available ACK on the product instance. See the **show license all**, **show license summary**, **show license status**, and **show license tech** commands in the command reference of the applicable release.
	CSLU support for Linux	CSLU can now be deployed on a machine (laptop or desktop) running Linux. See CSLU, on page 61, Workflow for Topology: Connected to CSSM Through CSLU, on page 86, and CSLU Disconnected from CSSM, on page 73.

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	RUM Report Throttling	For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases. See: Connected to CSSM Through CSLU, on page 69, Connected to CSSM Through CSLU, on page 69, CSLU Disconnected from CSSM, on page 73, and SSM On-Prem Deployment, on page 77.



CHAPTER 6

Management over Wireless

- Information About Management over Wireless, on page 181
- Restrictions on Management over Wireless, on page 181
- Enabling Management over Wireless on Controller (GUI) , on page 181
- Enabling Management over Wireless on Controller (CLI), on page 182

Information About Management over Wireless

The Management over Wireless feature allows operators to monitor and configure the controller using wireless clients connected to the wireless controller network.

Note By default, the Management over Wireless feature is disabled. You will need to keep the Management over Wireless feature disabled, if security is a concern.

This feature blocks the wireless management access to the same controller that the wireless client device is currently associated with. It does not prevent management access to a wireless client associated with another controller entirely. To completely block management access to wireless clients based on VLAN and so on, we recommend that you use Access Control Lists (ACLs) or a similar mechanism.

Restrictions on Management over Wireless

- The Management over Wireless feature does not work for Embedded Wireless Controller (EWC).

Enabling Management over Wireless on Controller (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Wireless Global**.

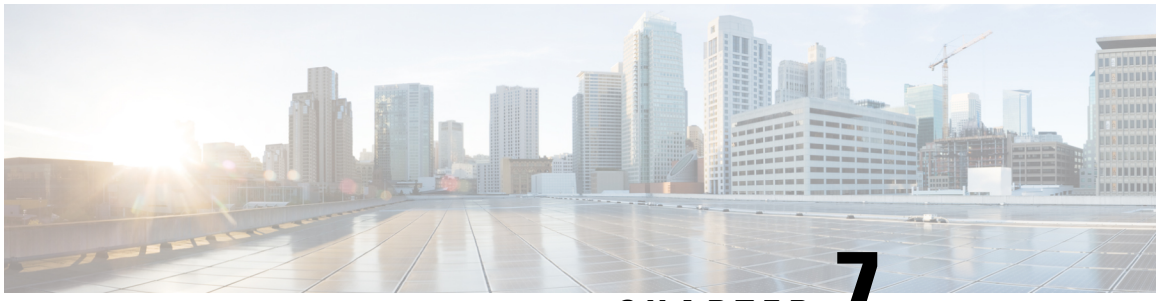
Step 2 Check the **Management via Wireless** check box.

Step 3 Click **Apply**.

Enabling Management over Wireless on Controller (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mgmt-via-wireless** **Example:** `Device(config)# wireless mgmt-via-wireless`	Enables management over wireless. Use the **no** form of this command to disable the management over wireless.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.



CHAPTER 7

Boot Integrity Visibility

- Overview of Boot Integrity Visibility, on page 183
- Verifying Software Image and Hardware, on page 183
- Verifying Platform Identity and Software Integrity, on page 184

Overview of Boot Integrity Visibility

Boot Integrity Visibility allows the Cisco platform identity and software integrity information to be visible and actionable. Platform identity provides the platform's manufacturing installed identity. Software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted trusted code.

During the boot process, the software creates a checksum record of each stage of the bootloader activities.

You can retrieve this record and compare it with a Cisco-certified record to verify if your software image is genuine. If the checksum values do not match, you may be running a software image that is either not certified by Cisco or has been altered by an unauthorized party.

Verifying Software Image and Hardware

This task describes how to retrieve the checksum record that was created during a switch bootup. Enter the following commands in privileged EXEC mode.

Note On executing the following commands, you might see the message **% Please Try After Few Seconds** displayed on the CLI. This does not indicate a CLI failure, but indicates setting up of underlying infrastructure required to get the required output. We recommend waiting for a few minutes and then try the command again.

The messages **% Error retrieving SUDI certificate** and **% Error retrieving integrity data** signify a real CLI failure.

Procedure

	Command or Action	Purpose
Step 1	**show platform sudi certificate** [**sign** [**nonce** *nonce*]]	Displays checksum record for the specific SUDI.

	Command or Action	Purpose
	Example: `Device# show platform sudi certificate sign nonce 123`	• (Optional) **sign** - Show signature. • (Optional) **nonce** - Enter a nonce value.
Step 2	**show platform integrity** [**sign** [**nonce** *nonce*]] **Example:** `Device# show platform integrity sign nonce 123`	Displays checksum record for boot stages. • (Optional) **sign** - Show signature. • (Optional) **nonce** - Enter a nonce value.

Verifying Platform Identity and Software Integrity

Verifying Platform Identity

The following example displays the Secure Unique Device Identity (SUDI) chain in PEM format. Encoded into the SUDI is the Product ID and Serial Number of each individual device such that the device can be uniquely identified on a network of thousands of devices. The first certificate is the Cisco Root CA 2048 and the second is the Cisco subordinate CA (ACT2 SUDI CA). Both certificates can be verified to match those published on https://www.cisco.com/security/pki/. The third is the SUDI certificate.

Important All the CLI outputs provided here are intended only for reference. The output differs based on the configuration of the device.

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
olEwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
```

```
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIEAwQD7zANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE4MDkyMzIyMzIwNloXDTI5
MDUxNDIwMjU0MVowaTEnMCUGA1UEBRMeUElEOkM5NjAwLVNVUC0xIFNOOkNBVDIy
MzZMMFE5MQ4wDAYDVQQKEwVDaXNjbzEYMBYGA1UECxMPQUNULTIgTGl0ZSBTVURJ
MRQwEgYDVQQDEwtDOTYwMC1TVVAtMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANsh0jcvgh1pdOjP9KnffDnDc/zEHDzbCTWPJi2FZcsaSE5jvq6CUqc4
MYpNAZU2Jym7NSD8iQbMXwbnCtoL64QtxQeFhRYmc4d5o933M7GwpEH0I7HUSbO/
Fxyp7JBmGPPgAkY7rKsYENiNK2hiR7Q2O7X2BidOKknEuofWdJMNyMaZgLYLOHbJ
5oXaORxhUy3VRaxNl6qI7kYxuugg2LcAbZ539sRXe8JtHyK8llURNSGMiQ0S17pS
idGmrJJ0pEHA0EUVTZqEny3z+NW9uxLVSzu6+hEJYlqfI+YEf0DbVZly1cy5r/jF
yNdGuGKvd5agvgCly8aYMZa3P+D5S8sCAwEAAaNvMG0wDgYDVR0PAQH/BAQDAgXg
MAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEEAQkVAgOgNRMzQ2hpcElE
PVUxUk5TVEl3TVRjd05qSTFBQUFwZndBQUFBQUFBQUFBQUFBQUFBQUhtSlU9MA0G
CSqGSIb3DQEBCwUAA4IBAQCrpHo/CUyk5Hs/asIcYW0ep8KocSkbNh8qamyd4oWD
e/MGJW9Bs5f09IEbILWPdytCCS2lSyJbxz2HvVDzdxQdxjDwUNiWuu3dWMXN/i67
yuCGM+lA1AAG5dT6lNgWYHh+YzsZm9eoq1+4NM+JuMXWsnzAK8rSy+dSpBxqFsBq
E0OlPsaK7y2h8gs+XrV9x+D48OZQkTRXpxhJfiWvs+EbdgsAM/vBxTAoTJPVmXWN
Cmcj9X52Xl3i4MdOUXocZLO2kh6JSgOYGkFeZifJ0iDvMfAf0cJ6+cEF6bSxAqBL
veel+8LmeiE/2O9h6qGHPPDacCaXA2oJCDHveAt8iPTG
-----END CERTIFICATE-----

Signature version: 1
Signature:
[redacted]
```

The optional RSA 2048 signature is across the three certificates, the signature version and the user-provided nonce.

```
RSA PKCS#1v1.5 Sign {<Nonce (UINT64)> || <Signature Version (UINT32)> || <Cisco Root CA
2048 cert (DER)> ||
<Cisco subordinate CA (DER)> || <SUDI certificate (DER)> }
```

Cisco management solutions are equipped with the ability to interpret the above output. However, a simple script using OpenSSL commands can also be used to display the identity of the platform and to verify the signature, thereby ensuring its Cisco unique device identity.

```
[linux-host:~]openssl x509 -in sudi_id.pem -subject -noout
subject= /serialNumber=PID:C9600-SUP-1 SN:CAT2239L06B/CN=C9600-SUP-1-70b3171eaa00
```

Verifying Software Integrity

The following example displays the checksum record for the boot stages. The hash measurements are displayed for each of the three stages of software successively booted. These hashes can be compared against

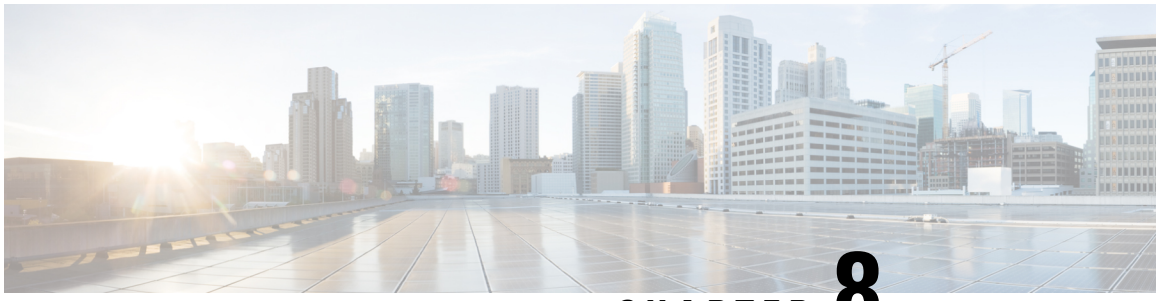
Cisco-provided reference values. An option to sign the output gives a verifier the ability to ensure the output is genuine and is not altered. A nonce can be provided to protect against replay attacks.

Note Boot integrity hashes are not MD5 hashes. For example, if you run **verify /md5 cat9k_iosxe.16.10.01.SPA.bin** command for the bundle file, the hash will not match.

The following is a sample output of the **show platform integrity sign nonce 123** command. This output includes measurements of each installed package file.

```
Device# show platform integrity sign nonce 123
Platform: C9800-L-F-K9
Boot 0 Version: R04.1173930452019-06-11
Boot 0 Hash: A6C92C44976FC77DD42234444FFD87798FB9036A2762FAA4999A190A0258B18C
Boot Loader Version: 16.12(1r)
Boot Loader Hash:
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
OS Version: 2020-03-19_20.26
OS Hashes:
C9800-L-universalk9_wlc.2020-03-19_20.26.SSA.bin:
53E2DF1A1A082E36FA4CAB817C1794EC9D69AC0E90BCCBFECF9BCD0BCA9385AA9E9372ABF7431E4A08FC5E5B9670131C09D158E5B8A7B457501FE77AB9F1C26D
C9800-L-mono-universalk9_wlc.2020-03-19_20.26.SSA.pkg:
1D3279D53B0311CE42C669824DF86FB5596CD7CA45CA8D7FDC3D10657B8C9A48F4B0508D7BCFFD645CB6571AC1E674A57A82414E3D6E1666BE64E6132F707671
PCR0: EE14A2D5099DA343B3941C54A429C4AC1D3EE8E9B609F1AC00049768A470734E
PCR8: 78794D0F5667F8FA4E425E3CA2AF3CD99B90B219FD90222D622B3D563416BBAA
```

Note Only OS and package hashes are supported.



CHAPTER 8

SUDI99 Certificate Support

- SUDI99 Certificate Support, on page 187
- Disabling SUDI99 Migration (GUI), on page 189

SUDI99 Certificate Support

Cisco Catalyst 9800 Series Wireless Controllers use Secure Unique Device Identity (SUDI) certificates as device certificates for authentication during secure connection handshakes. These certificates are provisioned in a secure hardware chip, which can hold multiple certificates, during the manufacturing process.

Note Some of the certificates used in the controller and AP platforms are expiring in May 2029 and require migration to a new set of certificates. SUDI99 certificate support is addressing this migration scenario. SUDI99 is valid until December 2099.

The Cisco IOS XE software supports two slots for initializing SUDI certificates from the secure hardware chip. This SUDI99 migration change will rearrange certificate-to-trustpoint mapping as follows:

Table 13: Existing Software Selection for SUDI Trustpoint Certificates

Trustpoint Name	Software Selection Among Programmed Certificate Chains
CISCO_IDEVID_SUDI	CMCA2 SHA2 SUDI (SHA2-2037)
CISCO_IDEVID_SUDI_LEGACY	CMCA SHA1 SUDI

Table 14: New Software Selection for SUDI Trustpoint Certificates

Trustpoint Name	Software Selection Among Programmed Certificate Chains
CISCO_IDEVID_SUDI	CMCA-III SHA2 SUDI99
CISCO_IDEVID_SUDI_LEGACY	CMCA2 SHA2 SUDI (SHA2-2037)

Caution Performing device authentication using expired certificates may lead to service disruption.

The following table lists the SUDI99 certificate and software support:

Table 15: SUDI99 Certificate and Software Support

Cisco Catalyst 9800 Controllers	SUDI99 Certificate Support	Software Support for SUDI99 Migration
Cisco Catalyst 9800-CL Wireless Controller for Cloud	Not supported.	—
Cisco Catalyst 9800 Series Wireless Controllers • 9800-40 • 9800-80 • 9800-L	Supported	Yes. From Cisco IOS XE Cupertino 17.7.1.
Cisco Embedded Wireless Controller on Catalyst Access Points. • 9105AXI • 9115AXI • 9115AXE • 9117AXI • 9120AXI • 9120AXE • 9120AXP • 9130AXI • 9130AXE	Supported	Yes. From Cisco IOS XE Cupertino 17.7.1.
Cisco Embedded Wireless Controller on Catalyst Switches • 9300 Series • 9400 Series • 9500 Series • 9500H Series	Not supported.	—

Backward Compatibility

The Cisco Catalyst 9800 Series Wireless Controllers have a default wireless management trustpoint. Some applications use this management trustpoint certificate. If a device (AP or controller) cannot validate the SUDI99 certificate, then the controller uses an older certificate (SHA2-2037) as its device certificate for that particular connection.

For NMSP-TLS connections with Cisco CMX, the client certificate is not validated in default security mode. However, in FIPS mode, Cisco CMX validates the controller certificate.

If Cisco CMX is deployed in FIPS mode, explicitly install the new SUDI CA certificates on the Cisco CMX running the earlier version of Cisco CMX or upgrade Cisco CMX to the latest version.

Some applications, such as HTTPS, RADSEC, and WebAuth, do not use SUDI certificate as their default trustpoint. But, it is possible to configure SUDI trustpoint explicitly in them. The SUDI refresh program alters the certificate selection for such services. However, there is no functional impact.

Restrictions

If a SUDI99 certificate is incorrectly programmed in a device, it is rejected during trustpoint initialization at bootup, and trutpoint-to-certificate mapping falls back to the old behaviour. User can verify the SUDI certificate status using the **show platform sudi pki** command.

Disabling SUDI99 Migration Using CLI

The SUDI99 certificate is set as the default trustpoint in supported hardware units. You can disable it using the **no platform sudi cmca3** command. In high availability (HA) deployments, form the HA pair, and then run the command. Then, save the configuration and reload the controller to disable the SUDI certificate and fall back to the older trustpoint certificate.

To check the certificate validation status, use the **show platform sudi pki** command.

Disabling SUDI99 Migration (GUI)

SHA1 SUDI certificates on hardware controllers have an imminent expiry date and devices using expired certificates face disruption in service. To ensure a smooth migration to the latest SUDI99 certificate issued by CMCA-III authority, the controllers have been programmed with newer certificates in their secure hardware chip. These certificates are enabled by default and are valid till December 2099.

Follow the procedure given below, if you do not wish to migrate at this point.

Procedure

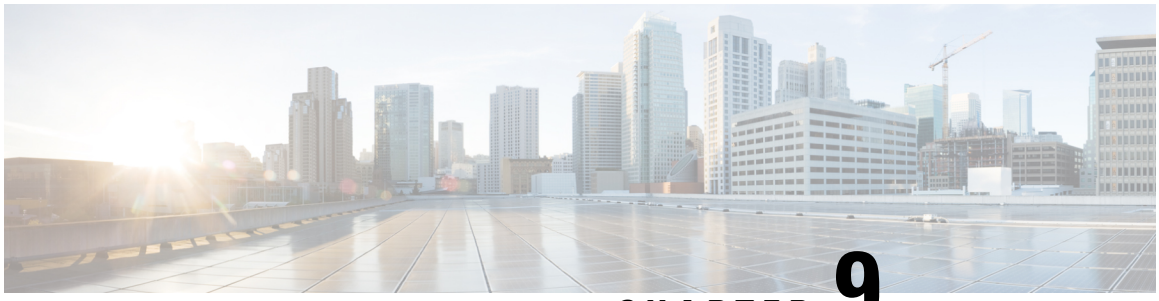
Step 1 On the **Configuration > Security > PKI Management > Trustpoint** tab, go to the **SUDI Status** section.

Step 2 Disable the **Cisco Manufacturing CA III certificate** to continue using the older certificate that is mapped to an existing Trustpoint.

Step 3 Click **Apply**

What to do next

Reload the device for the configuration to take effect.



CHAPTER 9

Link Aggregation Group

- Information About Link Aggregation Group, on page 191

Information About Link Aggregation Group

A link aggregation group (LAG) bundles all of the controller's distribution system ports into a single 802.3ad port channel. This reduces the number of IP addresses required to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the corresponding user.

LAG simplifies controller configuration because you no longer have to configure ports for each interface. If any of the controller ports fail, traffic is automatically migrated to one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

Note The wireless management VLAN can only be part of one port channel.

Note LACP is supported on a standalone controller from Cisco IOS XE Gibraltar 16.12.x release. LACP is supported on an SSO pair from Cisco IOS XE Amsterdam 17.1.1s onwards.

Link Aggregation Control Protocol

Link Aggregation Control Protocol (LACP) is a part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to a peer. By using the LACP, the wireless controller learns the identity of peers that are capable of supporting LACP, and the capabilities of each port. The LACP then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly, configured ports are grouped based on hardware, administrative, and port parameter constraints. If any of the controller ports fail, traffic is automatically migrated to one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

Configuring LAG Using LACP

To configure LAG using LACP, multiple port-channel interfaces must be created, and these interfaces should be added to the corresponding port bundle. LACP should also be configured on the uplink switch for the LACP bundle to come up.

- Create a port-channel interface
- Add interface to the port-channel
- Add VLAN to LAG
- Add interface to the port-channel

Port Aggregation Protocol

Port Aggregation Protocol (PAgP) is a Cisco-proprietary protocol that you can run on controllers. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports. PAgP packets are sent between Fast EtherChannel-capable ports in order to form a channel. When any of the active ports fail, a standby port becomes active.

By using PAgP, the controller learns the identity of partners that are capable of supporting PAgP and the capabilities of each port. PAgP then dynamically groups similarly configured ports (on a single device in a stack) into a single logical link (channel or aggregate port). Similarly, configured ports are grouped based on hardware, administrative, and port parameter constraints.

Configuring LAG Using PAgP

To configure LAG using PAgP, multiple port-channel interfaces must be created, and these interfaces should be added to the corresponding port bundle. PAgP should also be configured on the uplink switch for the PAgP bundle to come up.

- Create a port-channel interface
- Add interface to the port-channel

Information About Port Channel Interface Number

From Cisco IOS XE Bengaluru 17.5.1 onwards, the flexibility to number the port channel interface numbers between 1 and 64 is supported on the following Cisco Catalyst 9800 Series Wireless Controllers:

- Cisco Catalyst 9800-CL Wireless Controller for Cloud: The available range on the CLI is 1 to 64. The maximum supported port channel interfaces are 64.
- Cisco Catalyst 9800-L Wireless Controller: The available range on the CLI is 1 to 64. The maximum supported port channel interfaces are 14.
- Cisco Catalyst 9800-40 Wireless Controller: The available range on the CLI is 1 to 64. The maximum supported port channel interfaces are 16.
- Cisco Catalyst 9800-80 Wireless Controller: The available range on the CLI is 1 to 64. The maximum supported port channel interfaces are 64.

For example on the Cisco Catalyst 9800-L Wireless Controller, port-channel interface numbers can be anywhere between 1 and 64, as long as the total number of port-channel interfaces are 14 or lesser.

Note If you have configured 16 port-channel interfaces on the Cisco Catalyst 9800-40 Wireless Controller, and if the configured port-channel interfaces have reached their limitation, the following error message is displayed when you try to configure the 17th port-channel interface:

```
Device(config)#
Dec 15 08:58:22.209 CST: %ETC-5-CANNOT_ALLOCATE_AGGREGATOR: Aggregator limit reached, cannot
 allocate aggregator for group 17
```

When you downgrade from Cisco IOS XE Bengaluru 17.5.1 to an earlier version, and if the port channels are configured with a higher range than the supported range in the earlier version, the following errors are displayed when the earlier version is started. The non supported port channels disappear after the downgrade is completed.

```
interface Port-channel29
^% Invalid input detected at '^' marker.
interface Port-channel35
^% Invalid input detected at '^' marker.
```

Note that the HA pairing remains intact after downgrade.

Configuring LAG in ON Mode

To configure LAG in ON mode, multiple port-channel interfaces must be created, and these interfaces should be added to the corresponding port bundle. LACP should also be configured on the uplink switch for the LACP bundle to come up.

- #unique_237

Multichassis Link Aggregation Group

From Cisco IOS XE Amsterdam 17.2.1, Multichassis Link Aggregation Group (multi-LAG), which provides flexibility in connecting the controller to a switch's infrastructure is supported. Using multi-LAG, you can connect the multiple uplinks from the controller to the separated uplink switches. The controller supports VLAN-based traffic splitting when connected to a multiswitch topology. This provides the ability to distribute traffic on different uplinks, based on VLANs, for example, supporting a use case where guest traffic can be completely isolated to a different switch or network from the enterprise network. Same VLAN cannot be configured on both the uplinks.

You can connect a LAG to a single switch. However, different VLANs must be connected to different LAGs. The redundancy port must be connected to the same distribution switch as the uplinks, or back to back.

Multi-LAG is supported in LAG ON mode, LACP, and PAgP modes.

Prerequisites for Multi-LAG

- Each LAG must be connected to a single switch.
- Different VLANs must be assigned to different LAGs.

Restrictions for Multi-LAG

- If the primary LAG fails, automatic failover to secondary LAG is not supported.
- The interface on the controller does not come up when you shut or unshut the port on the switch port.

Note This is specific to Cisco Catalyst 9800-CL Cloud Wireless Controller in KVM environment for SR-IOV.

Supported Topologies

The Cisco Catalyst 9800-80 Wireless Controller has eight ports, while the Cisco Catalyst 9800-40 and Cisco Catalyst 9800-L wireless controllers have four ports each. You can create multi-LAGs of ports with similar capabilities, for example, 2.5 G and 2.5 G, or 10 G and 10 G. You cannot have a 2.5 G and a 10 G port in a port channel group with a minimum of two ports in one LAG.

Figure 14: Single Controller with Multi-LAG

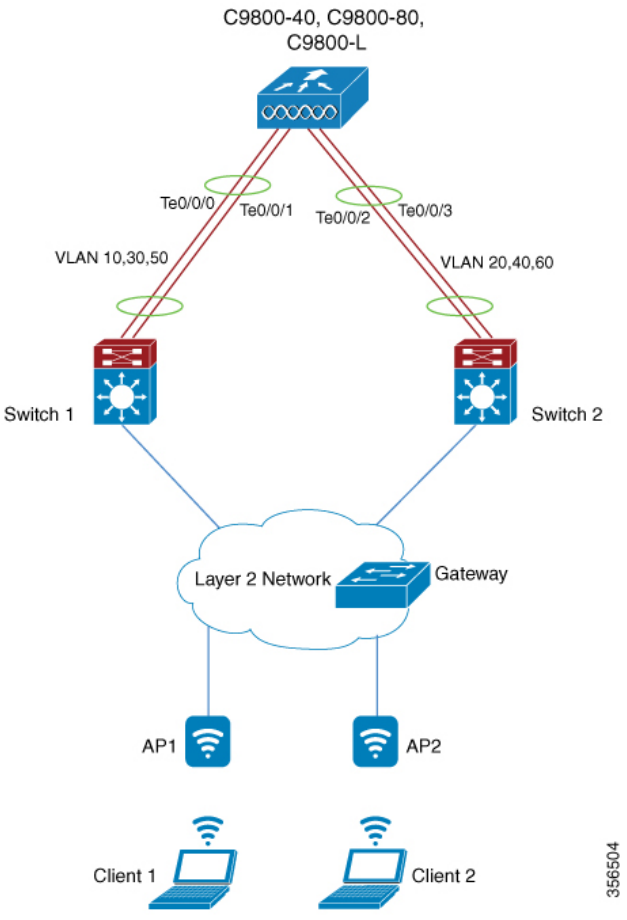
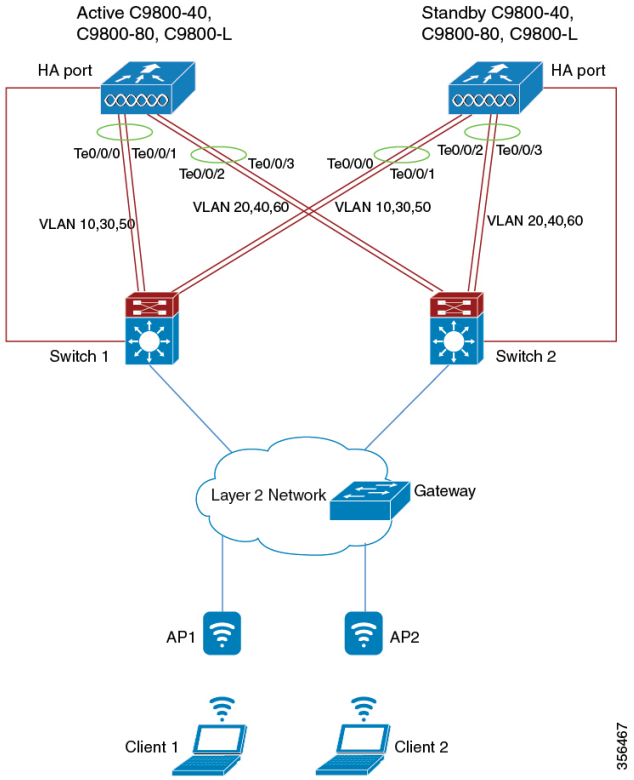


Figure 15: SSO Pair with Multi-LAG



Configuring a Port Channel Interface (GUI)

Procedure

Step 1 Choose **Configuration** > **Interface** > **Logical**.

Step 2 Click the **Port Channel** tab to configure the Port Channel interface.

The **Port Channel** tab lists all the logical port-channel interfaces on the device.

Step 3 Click **Add** to add to a new logical port channel interface.

The **Add Port Channel Interface** window is displayed.

Step 4 In the **Add Port Channel Interface** complete the following procedure:

a) In the **Port Channel Number** field, enter the port channel number. The valid values are between 1 to 64.
b) In the **Description** field, enter the port channel description.
c) Click the **Admin Status** toggle button to set the admin status as *UP* or *DOWN*.
d) Click the **Enable Layer 3 Address** toggle button to enable the Layer 3 address.
e) In the Port Members section, select the port members from the list displayed in the **Available** list box, and add it to the **Associated** list.
f) From the **Switchport Mode** drop-down list, choose a switch mode for the interface.

- If you choose *access* as the switch mode, enter the access VLAN ID in the **Access VLAN** field.
- If you choose *trunk* as the switch mode, enter the VLAN IDs that you want to assign as trunk links. To allow all VLAN IDs as trunk links, set the **Allowed VLANs** to **All**. Specify a native VLAN.
- If you choose *dynamic auto* or *dynamic desirable* as the switch mode, enter the access VLAN ID. Enter the VLAN IDs you want to assign as trunk links. To allow all VLAN IDs as trunk links, set the **Allowed VLANs** to All. Specify a native VLAN.

g) Click **Update & Apply to Device**.

Create a Port-Channel Interface

Follow the procedure given below to create a port-channel interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface port-channel** *port-channel* **Example:** `Device(config)# interface port-channel 2`	Configures the port channel and enters interface configuration mode. The valid values for the port channel number ranges from 1 to 64.
Step 3	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the port as trunk.
Step 4	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Enables the interface.

Configuring LAG in ON Mode

Follow the procedure given below to configure LAG in ON mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**interface TenGigabitEthernet** *port-slot* **Example:** `Device(config)# interface TenGigabitEthernet0/0/0`	Configures the port.
Step 3	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the port as trunk.
Step 4	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Disables the interface.
Step 5	**channel-group** *group-number* **mode on** **Example:** `Device(config-if)# channel-group 3 mode on`	Assigns the port to a channel group, and specifies the ON mode. The valid values for the port channel number ranges from 1 to 64.
Step 6	**switchport trunk allowed vlan** *vlan-id* **Example:** `Device(config-if)# switchport trunk allowed vlan 16,17`	Assigns the allowed VLAN ID to the port when it is in trunking mode.

Add an Interface to a Port Channel (LACP)

Follow the procedure given below to add an interface to a port channel using the LACP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface TenGigabitEthernet** *port-slot* **Example:** `Device(config)# interface TenGigabitEthernet0/0/0`	Configures the port.
Step 3	**channel-group** *group-number* {**active** | **passive**} **Example:** `Device(config-if)# channel-group 1 mode active`	Assigns the port to a channel group, and specifies the LACP mode. The valid values for the port channel number ranges from 1 to 64.

	Command or Action	Purpose
Step 4	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the port as trunk.

Add an Interface to a Port Channel (PAgP)

Follow the procedure given below to add an interface to a port channel using the PAgP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface TenGigabitEthernet** *port-slot* **Example:** `Device(config)# interface TenGigabitEthernet0/0/0`	Configures the TenGigabit Ethernet interface.
Step 3	**channel-group** *group-number* {**auto** | **desirable**} **Example:** `Device(config-if)# channel-group 1 mode auto`	Assigns the port to a channel group, and specifies the PAgP mode. The valid values for the port channel number ranges from 1 to 64.
Step 4	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the port as trunk.

Add a VLAN to a Port Channel

Follow the procedure given below to add different VLANs under a port channel.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface port-channel** *port-channel* **Example:**	Configures the port channel.

	Command or Action	Purpose
	`Device(config)# interface port-channel 1`	Valid values for the port channel number range from 1 to 64.
Step 3	**switchport trunk allowed vlan** *vlan-id* **Example:** `Device(config-if)# switchport trunk allowed vlan 10,30,50`	Adds VLANs to the list of allowed VLANs.

Remove a Port Channel Group from a Physical Interface

Perform this task to remove a port channel group from a physical port.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface TenGigabitEthernet** *port-slot* **Example:** `Device(config)# interface TenGigabitEthernet0/0/0`	Enters the TenGigabit Ethernet interface.
Step 3	**no channel-group** **Example:** `Device(config-if)# no channel-group`	Removes the port channel group from the physical port.
Step 4	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode.

Verify the LAG Configuration

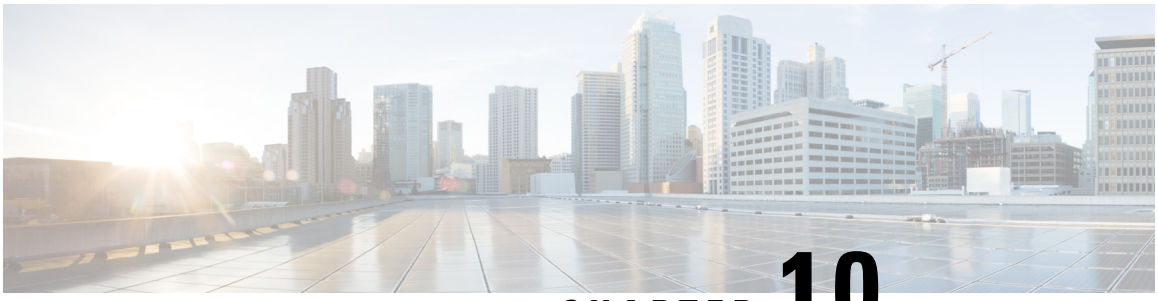
To view a port channel's state, use the following command:

```
Device# show etherchannel summary

Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
3      Po3(SU)         LACP        Tw0/0/0(P)      Tw0/0/1(P)
4      Po4(SU)         LACP        Tw0/0/2(P)      Tw0/0/3(P)
```

To verify an LACP or PAgP configuration, use the following commands:

```
Device# show running-config interface tenGigabitEthernet 0/0/0

Building configuration...

Current configuration : 114 bytes
!
interface TwoGigabitEthernet0/0/0
 switchport trunk allowed vlan 16,17
 switchport mode trunk
 speed 1000
 no negotiation auto
 no snmp trap link-status
 channel-group 3 mode on


Device# show running-config interface port-channel 1

Building configuration...

Current configuration : 54 bytes
!
interface Port-channel1
 switchport mode trunk
 switchport trunk allowed vlan 10,30,50
end
```



CHAPTER 10

Best Practices

- Introduction, on page 201

Introduction

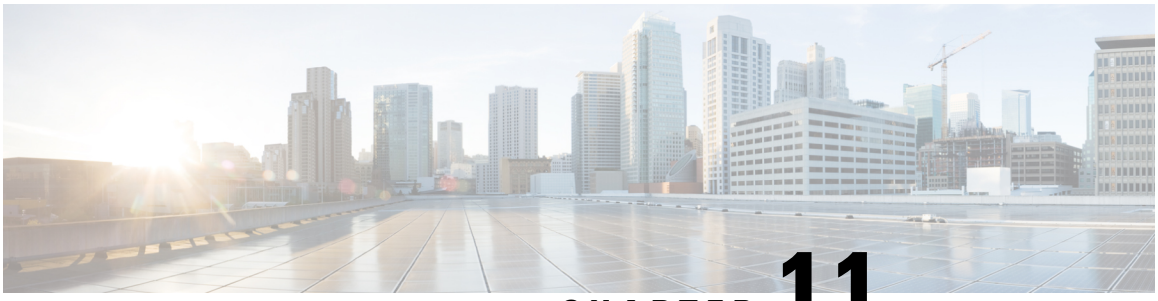
This chapter covers the best practices recommended for configuring a typical Cisco Catalyst 9800 Series wireless infrastructure. The objective is to provide common settings that you can apply to most wireless network implementations. However, not all networks are the same. Therefore, some of the tips might not be applicable to your installation. Always verify them before you perform any changes on a live network.

For more information, see Cisco Catalyst 9800 Series Configuration Best Practices guide.

PART II

System Upgrade

- Upgrading the Cisco Catalyst 9800 Wireless Controller Software, on page 205
- In-Service Software Upgrade, on page 213
- Software Maintenance Upgrade, on page 223
- Efficient Image Upgrade, on page 241
- Predownloading an Image to an Access Point, on page 247
- N+1 Hitless Rolling AP Upgrade, on page 255
- Site-Based Rolling AP Upgrade in N+1 Networks, on page 259
- NBAR Dynamic Protocol Pack Upgrade, on page 271
- Wireless Sub-Package for Switch, on page 273



CHAPTER 11

Upgrading the Cisco Catalyst 9800 Wireless Controller Software

- Overview of Upgrading the Controller Software, on page 205
- Upgrading the Controller Software (GUI), on page 206
- Upgrade the Controller Software (CLI), on page 207
- Converting From Bundle-Mode to Install-Mode, on page 208
- Copying a WebAuth Tar Bundle to the Standby Controller, on page 211

Overview of Upgrading the Controller Software

This section describes the upgrade process and the methods to upgrade the Cisco Catalyst 9800 Series Wireless Controller Software.

Newer versions of the controller software are released at regular intervals. This includes major releases as well as rebuild releases that focuses on bug fixes. The version of the AP software is also tied to the controller software release. Every major Cisco IOS XE software release contains new sets of features that are essential for the enterprise-class customers.

Each Cisco IOS XE software release is classified as either a Standard-Support release or an Extended-Support release.

Standard-Support Release

- A sustaining support lifetime of 12 months from First Customer Shipment (FCS) with two scheduled rebuilds
- Rebuilds are typically released at 6 months intervals after FCS.

Extended-Support release Details

- A sustaining support lifetime of 36 months from FCS with ten scheduled rebuilds.
- These rebuilds are at 3, 4, 4, 6, 7 months intervals after FCS or via SMU support. Last 12 months of support will be via SMU.

Based on your requirement, such as upgrading the full image or applying a software patch for bugs, you can go for an appropriate software upgrade, using either GUI or CLI.

- Upgrade the Controller Software (GUI)

- Upgrade the Controller Software (CLI)

Software Upgrade Options

- **Software Maintenance Upgrade**: This method installs a software package on the system to provide a patch fix or a security resolution to a released image. This upgrade package is provided on a per release and per component basis, and is specific to the platform.
- **Hitless Upgrade**: This method allows the APs to be upgraded in a staggered manner, while still being connected to the same controller. This avoids upgrade downtime even for N+1 networks.
- **In-Service Software Upgrade**: This method upgrades a wireless controller image to a later release while the network forwards packets. This feature is supported only within and between major releases.

Note We recommend In-Service Software Upgrade if you are upgrading the entire image or cold controller SMU. Use Software Maintenance Upgrade for software patches or bug fixes.

The software upgrade time is estimated to be less than 6 hours for a large network. However, the upgrade time depends on factors such as the number of APs, the percentage of APs to upgrade in each iteration, the controller type (9800-80, 9800-L, and so on), and the connectivity between the controller and the APs.

Device Upgrade Options

The following device upgrade options are available:

- NBAR Dynamic Protocol Pack Upgrade: Protocol packs are software packages that update the Network-Based Application Recognition (NBAR) engine protocol support on a device without replacing the Cisco software on the device. A protocol pack contains information on applications that are officially supported by NBAR, and are compiled and packed together.
- Field Programmable Upgrade: These are hardware programmable packages released by Cisco to upgrade the hardware programmable firmware. Hardware programmable package upgrade is necessary only when a system message indicates that one of the field programmable devices needs an upgrade or when a Cisco technical support representative suggests an upgrade.

Upgrading the Controller Software (GUI)

Before you begin

Clean up the old installation files using the **Remove Inactive Files** link.

Note For GUI options such as *Software Maintenance Upgrade*, *AP Service Package*, and *AP Device Package*, see the respective feature sections.

Procedure

Step 1 Choose **Administration** > **Software Management** .

Step 2 Choose an option from the **Upgrade Mode** drop-down list:

- **INSTALL**: The Install mode uses a package-provisioning file named *packages.conf* in order to boot a device.
- **BUNDLE**: The Bundle mode uses monolithic Cisco IOS images to boot a device. The Bundle mode consumes more memory than the Install mode because the packages are extracted from the bundle and copied to RAM.

Note You get to view the **Destination** field only for BUNDLE upgrade mode.

Step 3 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as **TFTP**, **SFTP**, **FTP**, **Device**, or **Desktop (HTTP)**.

- If you choose **TFTP** as the **Transport Type**, enter the **Server IP Address** of the TFTP server that you want to use. Also, enter the complete **File Path**.

  In controllers, the IP TFTP source is mapped to the service port by default.
- If you choose **SFTP** as the **Transport Type**, enter the **Server IP Address** of the SFTP server that you want to use. Also, enter the **SFTP Username**, **SFTP Password**, and the complete **File Path**.
- If you choose **FTP** as the **Transport Type**, enter the **Server IP Address** of the FTP server that you want to use. Also, enter the **FTP Username**, **FTP Password**, and the complete **File Path**.
- If you choose **Device** as the **Transport Type**, choose the **File System** from the drop-down list. In the **File Path** field, browse through the available images or packages from the device and select one of the options, and click **Select**.
- If you choose **Desktop (HTTPS)** as the **Transport Type**, choose the **File System** from the drop-down list. In the **Source File Path** field, click **Select File** to select the file, and click **Open**.

Step 4 Click **Download & Install**.

Step 5 To boot your device with the new software image, click **Save Configuration &Activate**.

Step 6 Click **Commit** after the device reboots to make the activation changes persistent across reloads.

Note For 17.4 and later releases, this step is mandatory for the upgrade to be persistent. If you do not click **Commit**, the auto-timer terminates the upgrade operation after 6 hours, and the controller reverts back to the previous image.

Upgrade the Controller Software (CLI)

Before you begin

- Determine the Cisco IOS release that is currently running on your controller, and the filename of the system image using the **show version** command in user EXEC or privileged EXEC mode.

- Clean up the old installation files using the **install remove inactive** command.
- Use the **show version | include Installation mode** to verify the boot mode.

Note We recommend that you use install mode for the software upgrade.

For steps on converting the device from bundle-mode to install-mode, see Converting from Bundle-Mode to Install-Mode.

Procedure

Step 1 Download the software from Cisco.com: https://software.cisco.com/download/home/286322524

a) Click IOS XE Software link.

b) Select the release number you want to install, for example Gibraltar-16.12.3.

Note Cisco recommended release is selected by default. For release designation information, see: https://software.cisco.com/download/static/assets/i18n/reldesignation.html?context=sds

c) Click **Download**.

Step 2 Copy the new image to flash using the command: **copy tftp:***image* **flash:**

Step 3 Verify that the image has been successfully copied to flash using the command: **dir flash:**

Step 4 Upgrade the software by choosing an upgrade process from the options that are currently supported.

For a list of upgrade options, see Software Upgrade Options, on page 206.

Converting From Bundle-Mode to Install-Mode

Use the procedure given below to boot in install-mode:

Before you begin

- Clean up the old installation files using the command**install remove inactive**
- Verify the boot mode using the command: **show version | include Installation mode**
- Download the software image from Cisco.com.

  For steps on how to download the software, see *Upgrading the Controller Software (CLI)* .

Procedure

Step 1 Copy the new image to flash using the command: **copy tftp:***image* **flash:**

```
Device# copy tftp://xx.x.x.x//C9800-universalk9_wlc.xx.xx.xx.SSA.bin flash:
```

```
Destination filename [C9800-universalk9_wlc..xx.xx.xx..SSA.bin]?
Accessing tftp://xx.x.x.x//C9800-universalk9_wlc.xx.xx.xx.SSA.bin...
Loading /C9800-universalk9_wlc.xx.xx.xx.SSA.bin from xx.x.x.x (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]
601216545 bytes copied in 50.649 secs (11870255 bytes/sec)
```

Step 2 Verify that the image has been successfully copied to flash using the command: **dir flash:**

```
Device# dir flash:*.bin

Directory of bootflash:/*.bin

On Active

Directory of bootflash:/

   12  -rw-  1231746613  Jun 11 2020 23:15:49 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200611_101837.SSA.bin
   17  -rw-  1232457039   Jun 9 2020 21:14:40 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200609_031801.SSA.bin
   21  -rw-  1219332990  Jun 10 2020 02:06:14 +00:00
C9800-universalk9_wlc.BLD_V173_THROTTLE_LATEST_20200608_003622_V17_3_0_183.SSA.bin
   18  -rw-  1232167230   Jun 8 2020 02:42:22 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200607_002322.SSA.bin
24811823104 bytes total (16032391168 bytes free)


On Standby
Directory of stby-bootflash:/*.bin

Directory of stby-bootflash:/

   18  -rw-  1232167230   Jun 8 2020 02:42:22 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200607_002322.SSA.bin
   20  -rw-  1231746613  Jun 11 2020 23:15:49 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200611_101837.SSA.bin
   17  -rw-  1232457039   Jun 9 2020 21:14:40 +00:00
C9800-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20200609_031801.SSA.bin
   16  -rw-  1219332990  Jun 10 2020 02:06:14 +00:00
C9800-universalk9_wlc.BLD_V173_THROTTLE_LATEST_20200608_003622_V17_3_0_183.SSA.bin
26462998528 bytes total (17686335488 bytes free)
```

Step 3 Set the boot variable to **bootflash:packages.conf**.

```
Device(config)# boot sys flash bootflash:packages.conf
```

Step 4 Save your changes by entering this command: **write memory**.

```
Device(config)# write memory
```

Step 5 Verify whether the boot variable is set to bootflash:packages.conf using the command:**show boot**

```
Device# show boot

BOOT variable = bootflash:packages.conf,12;
CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x2102

Standby BOOT variable = bootflash:packages.conf,12;
Standby CONFIG_FILE variable =
```

```
Standby BOOTLDR variable does not exist
Standby Configuration register is 0x2102
```

Step 6 Move the device from bundle-mode to install-mode using the command: **install add file** *image.bin location* **activate commit**

```
Device# install add file bootflash:C9800-universalk9_wlc.xx.xx.xx.SPA.bin activate commit

install_add_activate_commit: START Thu Dec 6 15:43:57 UTC 2018
Dec 6 15:43:58.669 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin
install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin to the selected
chassis
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
[1] Add package(s) on chassis 1
[1] Finished Add on chassis 1
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: xx.xx.xx.216
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/C9800-xx-rpboot.xx.xx.xx.SPA.pkg
/bootflash/C9800-xx-mono-universalk9.xx.xx.xx.SPA.pkg
This operation requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on chassis 1
--- Starting list of software package changes ---
Old files list:
Removed C9800-xx-mono-universalk9.BLD_Vxxxx_THROTTLE_LATEST_20181022_153332.SSA.pkg
Removed C9800-xx-rpboot.BLD_Vxxxx_THROTTLE_LATEST_20181022_153332.SSA.pkg
New files list:

Added C9800-xx-mono-universalk9.xx.xx.xx.SPA.pkg
Added C9800-xx-rpboot.xx.xx.xx.SPA.pkg
Finished list of software package changes
[1] Finished Activate on chassis 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
[1] Commit package(s) on chassis 1
[1] Finished Commit on chassis 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Thu Dec 6 15:49:21 UTC 2018
Dec 6 15:49:21.294 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin
```

Note The system reloads automatically after executing the **install add file activate commit** command. You do not have to manually reload the system.

If upgrade fails, cleanup is required before attempting the upgrade procedure again. An upgrade failure may occur due lack of disk space, validation failure of extracted image, system crashes, and so on. Should a system failure occurs during upgrade process, wait till the system is back in service and check the system image version.

- If it is a new image, check for the stability and functionality of the system, and decide whether to commit and complete the upgrade procedure or discard the upgrade procedure.
- If it is a new image, use the cleanup procedure and reattempt the upgrade procedure.

Step 7 Click **yes** to all the prompts.

Step 8 Verify the boot mode using the command: **show version**

```
Device# show version | in Installation mode is

Installation mode is INSTALL
```

Copying a WebAuth Tar Bundle to the Standby Controller

Use the following procedure to copy a WebAuth tar bundle to the standby controller, in a high-availability configuration.

Procedure

Step 1 Choose **Administration > Management > Backup & Restore**.

Step 2 From the **Copy** drop-down list, choose **To Device**.

Step 3 From the **File Type** drop-down list, choose **WebAuth Bundle**.

Step 4 From the **Transfer Mode** drop-down list, choose **TFTP**, **SFTP**, **FTP**, or **HTTP**.

The **Server Details** options change based on the file transfer option selected.

- **TFTP**
  - **IP Address (IPv4/IPv6)**: Enter the server IP address (IPv4 or IPv6) of the TFTP server that you want to use.
  - **File Path**: Enter the file path. The file path should start with slash a (/*path*).
  - **File Name**: Enter a file name.

    The file name should not contain spaces. Underscores (_) and hyphen (-) are the only special characters that are supported. Ensure that file name ends with .tar, for example, webauthbundle.tar.

- **SFTP**
  - **IP Address (IPv4/IPv6)**: Enter the server IP address (IPv4 or IPv6) of the SFTP server that you want to use.

- **File Path**: Enter the file path. The file path should start with slash a (*/path*).
- **File Name**: Enter a file name.

  The file name should not contain spaces. Underscores (_) and hyphen (-) are the only special characters that are supported. Ensure that file name ends with .tar, for example, webauthbundle.tar.
- **Server Login UserName**: Enter the SFTP server login user name.
- **Server Login Password**: Enter the SFTP server login passphrase.

- **FTP**
  - **IP Address (IPv4/IPv6)**: Enter the server IP address (IPv4 or IPv6) of the TFTP server that you want to use.
  - **File Path**: Enter the file path. The file path should start with slash a (*/path*).
  - **File Name**: Enter a file name.

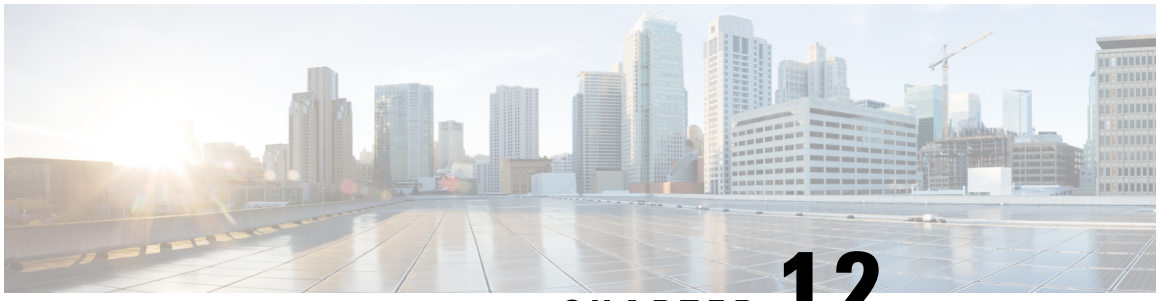
    The file name should not contain spaces. Underscores (_) and hyphen (-) are the only special characters that are supported. Ensure that file name ends with .tar, for example, webauthbundle.tar.
  - **Logon Type**: Choose the login type as either **Anonymous** or **Authenticated**. If you choose **Authenticated**, the following fields are activated:
    - **Server Login UserName**: Enter the FTP server login user name.
    - **Server Login Password**: Enter the FTP server login passphrase.

- **HTTP**
  - **Source File Path**: Click **Select File** to select the configuration file, and click **Open**.

Step 5 Click the **Yes** or **No** radio button to back up the existing startup configuration to Flash.

Save the configuration to Flash to propagate the WebAuth bundle to other members, including the standby controller. If you do not save the configuration to Flash, the WebAuth bundle will not be propagated to other members, including the standby controller.

Step 6 Click **Download File**.



CHAPTER 12

In-Service Software Upgrade

- Information About In-Service Software Upgrade, on page 213
- Prerequisites for Performing In-Service Software Upgrade, on page 214
- Guidelines and Restrictions for In-Service Software Upgrade, on page 214
- Upgrading Software Using In-Service Software Upgrade , on page 215
- Upgrading Software Using ISSU (GUI), on page 216
- Upgrading Software Using In-Service Software Upgrade with Delayed Commit, on page 217
- Monitoring In-Service Software Upgrade, on page 218
- Troubleshooting ISSU, on page 220

Information About In-Service Software Upgrade

In-Service Software Upgrade (ISSU) is a procedure to upgrade a wireless controller image to a later release while the network continues to forward packets. ISSU helps network administrators avoid a network outage when performing a software upgrade.

ISSU can also be used to apply cold patches without impacting the active network.

ISSU is supported only on the following Cisco Catalyst 9800 Series Wireless Controllers, and supports only upgrade.

- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-L Wireless Controller
- Cisco Catalyst 9800-CL Wireless Controller (Private Cloud)

High-Level Workflow of ISSU

1. Onboard the controller software image to the flash memory.
2. Download the AP image to the AP.
3. Install the controller software image.
4. Commit the changes.

Prerequisites for Performing In-Service Software Upgrade

- Ensure that both Active and Standby controllers are in install mode and are booted from *bootflash:/packages.conf*.
- Ensure that the network or device is not being configured during the upgrade.
- Schedule the upgrade when your network is stable and steady.
- Ensure uninterrupted power supply. A power interruption during upgrade procedure might corrupt the software image.

Guidelines and Restrictions for In-Service Software Upgrade

- If you do not run the **install commit** command within 6 hours of the **install activate issu** command, the system will revert to the original commit position. You can choose to delay the commit using the Delayed Commit procedure.
- During ISSU upgrade, while AP rolling upgrade is in progress, the **install abort** command won't work. You should use the **install abort issu** command, instead to cancel the upgrade.
- During ISSU upgrade, the system displays a warning message similar to:

  `found 46 disjoint TDL objects`

  . You can ignore the warning message because it doesn't have any functional impact.
- During ISSU upgrade, if both the controllers (active and standby) have different images after the power cycle, an auto cancel of ISSU is triggered to bring both the controllers to the same version. The following is a sample scenario: Install Version1 (V1) software on the active controller and then apply a SMU hot patch and perform a commit. Now, upgrade the software to Version2 using ISSU, and then power cycle the active controller. At this point, the system has a version mismatch (V1 and V2). The active controller reloads at this stage, after the completion of bulk synchronization. Now, both the controllers come up with the same version (V1 and V1).
- An ISSU upgrade that is canceled because of configuration synchronization failure on the standby controller rolls back to V1 of the software image. However, this information isn't available in the **show install** command log. Run the **show issu state detail** command to see the current ISSU state.
- To enable the **clear install** command, you should first run the **service internal** command in global configuration mode, and then run the **clear install** command in privileged EXEC mode.
- Image rollback could be affected if the controller has a stale rollback history and the stack gets formed afterwards. We recommend that you run the **clear install state** command to clear stale information and boot the controller in bundle mode.
- The **clear install state** command doesn't delete the SMU file from flash or storage. To remove a SMU, use either the **install remove file** command or the **install remove inactive** command.
- When the new active controller comes up, after the image upgrade, it doesn't retain the old logs on web GUI window as part of show logs.

- If a stateful switchover (SSO) or a high-availability (HA) event occurs during the rolling AP upgrade procedure of the ISSU feature, the rolling AP upgrade stops. You should then use the **ap image upgrade** command to restart the upgrade process.
- If HA fails to form after the ISSU procedure, you should reload any one chassis again to form HA again.
- Use clear **ap predownload statistics** command before using the **show ap image** command. This ensures that you get the right data after every pre-download.
- Manually cancel the ISSU process using the **install issu abort** command in the scenarios given below, to avoid a software version mismatch between the active controller and the standby controller.
  - An RP link is brought down after standby HOT during an ISSU procedure and the links remains down even after the auto-abort timer expiry.
  - An RP link is brought down before the standby controller reaches standby HOT during an ISSU procedure.
- Cisco TrustSec (CTS) is not supported on the RMI interfaces.
- If a switchover occurs while performing an AP upgrade using ISSU, the upgrade process will restart automatically after the switchover.

Upgrading Software Using In-Service Software Upgrade

Use the following procedure to perform a complete image upgrade, that is, from one image to another.

Note ISSU is supported only within and between major releases, for example, 17.3.*x* to 17.3.*y*, 17.6.*x* to 17.6.*y* (within a major release) and 17.3.*x* to 17.6.*x*, 17.3.*x* to 17.9.*x* (among major releases), that is, for two releases after the current supported release. ISSU is NOT supported within and between minor releases or between minor and major releases, for example 17.4.*x* to 17.4.*y* or 17.4.*x* to 17.5.*x* or 17.3.*x* to 17.4.*x*.

ISSU downgrade is not supported for Cisco Catalyst 9800 Series Wireless Controller platforms.

Note We recommend that you configure the percentage of APs to be upgraded by using the **ap upgrade staggered** command.

Procedure

	Command or Action	Purpose
Step 1	**install add file** *file-name* **Example:**	The controller software image is added to the flash and expanded.

	Command or Action	Purpose
	`Device# install add file <>`	**Note** In Cisco Catalyst 9800 Wireless Controller for Switch, run the **install add file** *sub-package-file-name* command to expand the wireless subpackage file.
Step 2	**ap image predownload** **Example:** `Device# ap image predownload`	Performs predownload of the AP image. To see the progress of the predownload, use the **show ap image** command.
Step 3	**install activate issu** [**auto-abort-timer** *timer*] **Example:** `Device# install activate issu`	Runs compatibility checks, installs the package, and updates the package status details. Optionally, you can configure the time limit to cancel the addition of new software without committing the image. Valid values are from 30 to 1200 minutes.

Step 4	Run either of the following commands:
	• **install abort issu**
	`Device# install abort issu`
	Cancels the upgrade process and returns the device to the previous installation state. This is applicable for both controller and the AP.
	• **install commit**
	`Device# install commit`
	Commits the activation changes to be persistent across reloads.
	Note If you do not run the **install commit** command within 6 hours of completing the previous step, the system will revert to the original commit position.	

Upgrading Software Using ISSU (GUI)

Before you begin

1. The device should be in Install mode.
2. The device should have an HA pair. The standby controller should be online and is in SSO mode.

You can verify the details using **show issu state detail** command.

Procedure

Step 1 Choose **Administration > Software Management**.

Step 2 Under the **Software Upgrade** tab, check the **ISSU Upgrade (HA Upgrade) (Beta)** check box.

Step 3 In the **AP Upgrade Configuration** section, from the **AP Upgrade per Iteration** drop-down list choose the percentage of APs to be upgraded.

Step 4 Click **Download & Install**.

This initiates the upgrade process and you can view the progress in the **Status** dialog box.

Click the **Show Logs** link to view the upgrade process details.

Note An SSO takes place while activating the image on the active controller. After the SSO, you should login again to the controller.

Step 5 The system enables the **Commit** and **ISSU Abort** buttons after the upgrade.

Click **Commit** to commit the activation changes, or **ISSU Abort** to terminate the upgrade process and return the device to the previous installation state.

Upgrading Software Using In-Service Software Upgrade with Delayed Commit

Use this procedure to upgrade the controller software with delayed commit, which will help you to run and test the new software without committing the image.

Procedure

	Command or Action	Purpose
Step 1	**install add file** *file-name* **Example:** `Device# install add file <file>`	Adds and expands the controller software image to the flash. **Note** In Cisco Catalyst 9800 Wireless Controller for Switch, run the **install add file** *sub-package-file-name* command to expand the wireless subpackage file.
Step 2	**ap image predownload** **Example:** `Device# ap image predownload`	Performs predownload of the AP image.

	Command or Action	Purpose
Step 3	**install auto-abort-timer stop** **Example:** `Device# install auto-abort-timer stop`	Stops the termination timer so that the upgrade process is not terminated after the default termination time of 6-8 hours.
Step 4	**install activate issu** **Example:** `Device# install activate issu`	Runs compatibility checks, installs the package, and updates the package status details.
Step 5	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads.

Monitoring In-Service Software Upgrade

To view the ISSU state after the install add ISSU and before the install activate ISSU, use the following command:

```
Device# show issu state detail

-- Starting local lock acquisition on chassis 1 ---
Finished local lock acquisition on chassis 1
Current ISSU Status: Enabled
Previous ISSU Operation: Abort Successful
=====================================================
System Check Status
-----------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
=====================================================
No ISSU operation is in progress
show install summary
[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG I 17.1.1.0.432
IMG C 16.12.2.0.2707
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

To view the ISSU state after activating ISSU, use the following command:

```
Device# show issu state detail

Current ISSU Status: In Progress
Previous ISSU Operation: Abort Successful
=====================================================
```

```
System Check Status
-------------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
=======================================================
Operation type: Step-by-step ISSU
Install type : Image installation using ISSU
Current state : Activated state
Last operation: Switchover
Completed operations:
Operation Start time
-------------------------------------------------------
Activate location standby Chassis 2 2019-09-17:23:41:12
Activate location active Chassis 1 2019-09-17:23:50:06
Switchover 2019-09-17:23:52:03
State transition: Added -> Standby activated -> Active switched-over
Auto abort timer: automatic, remaining time before rollback: 05:41:53
Running image: bootflash:packages.conf
Operating mode: sso, terminal state reached
show install summary
[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG U 17.1.1.0.432
--------------------------------------------------------------------------------
Auto abort timer: active on install_activate, time before rollback - 05:41:49
--------------------------------------------------------------------------------
```

To view the ISSU state after installing the commit, use the following command:

```
Device# show issu state detail

--- Starting local lock acquisition on chassis 1 ---
Finished local lock acquisition on chassis 1
Current ISSU Status: Enabled
Previous ISSU Operation: Successful
=======================================================
System Check Status
-------------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
=======================================================
No ISSU operation is in progress
show install summary
[ Chassis 1/R0 2/R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG C 17.1.1.0.432
--------------------------------------------------------------------------------
Auto abort timer: inactive
```

```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

To view the ISSU state after terminating the ISSU process, use the following command:

```
Device# show issu state detail
Current ISSU Status: In Progress
Previous ISSU Operation: Abort Successful
=====================================================
System Check Status
-----------------------------------------------------
Platform ISSU Support Yes
Standby Online Yes
Autoboot Enabled Yes
SSO Mode Yes
Install Boot Yes
Valid Boot Media Yes
=====================================================
Operation type: Step-by-step ISSU
Install type : Image installation using ISSU
Current state : Timeout-error state
Last operation: Commit Chassis 1
Completed operations:
Operation Start time
-----------------------------------------------------
Activate location standby Chassis 2 2019-09-17:23:41:12
Activate location active Chassis 1 2019-09-17:23:50:06
Switchover 2019-09-17:23:52:03
Abort 2019-09-18:00:14:13
Commit Chassis 1 2019-09-18:00:28:23
State transition: Added -> Standby activated -> Active switched-over -> Activated ->
Timeout-error
Auto abort timer: inactive
Running image: bootflash:packages.conf
Operating mode: sso, terminal state reached
```

To view the summary of the active packages in a system, use the following command:

```
Device# show install summary

[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG C 16.12.2.0.2707
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

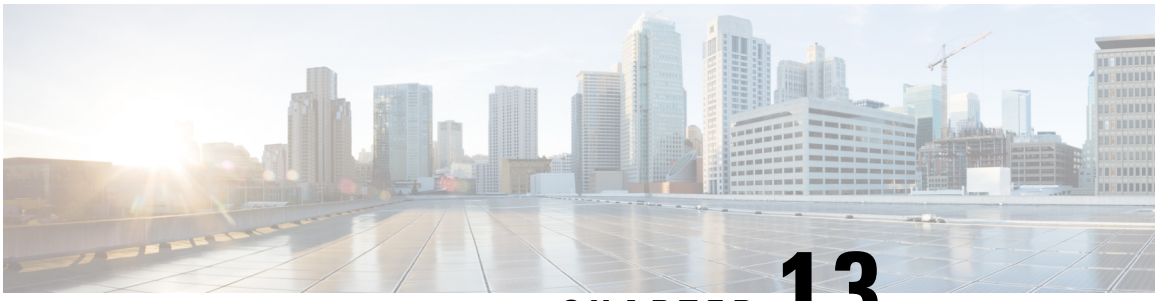
Troubleshooting ISSU

Using **install activate issu** command before completing AP pre-download.

The following scenario is applicable when you run the **install activate issu** command before completing AP pre-download. In such instances, you should run the **ap image predownload** command and then proceed with the activation.

```
Device# install activate issu
```

```
install_activate: START Wed Jan  8 04:48:04 UTC 2020
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]
y
Building configuration...
[OK]Modified configuration has been saved
install_activate: Activating ISSU
NOTE: Going to start Activate ISSU install process
STAGE 0: System Level Sanity Check
================================================
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
--- Verifying Platform specific ISSU admission criteria ---
CONSOLE: FAILED: Install operation is not allowed.
 Reason -> AP pre-image download is mandatory f
or hitless software upgrade.
 Action -> Trigger AP pre-image download.
FAILED: Platform specific ISSU admission criteria
ERROR: install_activate  exit(2 ) Wed Jan  8 04:48:37 UTC 2020
```



CHAPTER 13

Software Maintenance Upgrade

- Introduction to Software Maintenance Upgrade, on page 223
- Information About AP Device Package, on page 228
- Information About Per Site or Per AP Model Service Pack (APSP), on page 231

Introduction to Software Maintenance Upgrade

Software Maintenance Upgrade (SMU) is a package that can be installed on a system to provide a patch fix or a security resolution to a released image. A SMU package is provided for each release and per component basis, and is specific to the corresponding platform.

A SMU provides a significant benefit over classic Cisco IOS software because it allows you to address the network issue quickly while reducing the time and scope of the testing required. The Cisco IOS XE platform internally validates the SMU compatibility and does not allow you to install noncompatible SMUs.

All the SMUs are integrated into the subsequent Cisco IOS XE software maintenance releases. A SMU is an independent and self-sufficient package and does not have any prerequisites or dependencies. You can choose which SMUs to install or uninstall in any order.

Note SMUs are supported only on Extended Maintenance releases and for the full lifecycle of the underlying software release.

Note You can activate the file used in the **install add file** command only from the filesystems of the active device. You cannot use the file from the standby or member filesystems; the **install add file** command will fail in such instances.

Note When the SMU file is deleted and a reboot is performed, the device may display the following error message:

```
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
    FAILED: Improper State./bootflash/<previously-installed-smu-filename>.smu.bin not
present. Please restore file for stability.
Checking status of SMU_ADD on [1/R0]
SMU_ADD: Passed on []. Failed on [1/R0]
Finished SMU Add operation
FAILED: add_activate_commit /bootflash/<tobeinstalled-wlc-smu-filename>.smu.bin Wed Aug 02
 08:30:18 UTC 2023.
```

This error occurs because the previous SMU file was not properly removed from the controller. It may lead to functional errors, such as the inability to install new SMU or APSP files.

We recommend that you use the install remove file command to remove previous instances of APSP or SMU files from the bootflash.

SMU infrastructure can be used to meet the following requirements in the wireless context:

- Controller SMU: Controller bug fixes or Cisco Product Security Incident Response information (PSIRT).
- APSP: AP bug fixes, PSIRTs, or minor features that do not require any controller changes.
- APDP: Support for new AP models without introduction of new hardware or software capabilities.

Note The **show ap image** command displays cumulative statistics regarding the AP images in the controller. We recommend that you clear the statistics using the **clear ap predownload statistics** command, before using the **show ap image** command, to ensure that correct data is displayed.

SMU Workflow

The SMU process should be initiated with a request to the SMU committee. Contact your customer support to raise an SMU request. During the release, the SMU package is posted on the Cisco Software Download page and can be downloaded and installed.

SMU Package

An SMU package contains the metadata and fix for the reported issue the SMU is requested for.

SMU Reload

The SMU type describes the effect on a system after installing the corresponding SMU. SMUs can be nontraffic-affecting or can result in device restart, reload, or switchover.

A controller cold patch require a cold reload of the system during activation. A cold reload is the complete reload of the operating system. This action affects the traffic flow for the duration of the reload (~5 min). This reload ensures that all the processes are started with the correct libraries and files that are installed as part of the corresponding SMU.

Controller hot patching support allows the SMU to be effective immediately after activation, without reloading the system. After the SMU is committed, the activation changes are persistent across reloads. Hot patching

SMU packages contain metadata that lists all processes that need to be restarted in order to activate the SMU. During SMU activation, each process in this list will be restarted one at a time until the SMU is fully applied.

Installing a SMU (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management** and click the **Software Maintenance Upgrade** tab.

Step 2 Click **Add** to add a SMU image.

Step 3 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as TFTP, SFTP, FTP, Device, or Desktop (HTTP).

a) If you choose **TFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose a **File System** from the drop-down list. For example, if the SMU file is at the root of the TFTP server you can enter `/C9800-universalk9_wlc.17.03.02a.CSCvw55275.SPA.smu.bin` in the **File path** field.

b) If you choose **SFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and choose a **File System** from the drop-down list.

c) If you choose **FTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and choose a **File System** from the drop-down list.

d) If you choose **Device** as the **Transport Type**, you need to enter the **File path** and choose a **File System** from the drop-down list. This is possible when the software is already present on the device due to an earlier download and activation, followed by a subsequent deactivation.

Note The File System depends upon the kind of device you are using. On physical controllers, you have the option to store the file to the bootflash or hard disk, whereas in case of virtual controllers, you can only store it in the bootflash.

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose a **File System** from the drop-down list and click **Select File** to navigate to the **Source File Path**.

Step 4 Enter the **File Name** and click **Add File**.

This operation copies the maintenance update package from the location you selected above to the device and performs a compatibility check for the platform and image versions and adds the SMU package for all the members. After a SMU is successfully added to the system, a message is displayed about the successful operation and that the SMU can be activated on the device. The message displays the name of the package (SMU) that is now available to be activated. It lists the SMU Details - Name, Version, State (active or inactive), Type (reload, restart, or non-reload) and other compatibility details. If SMU is of the Type - reload, then any operation (activate, deactivate or rollback) will cause the device to reload; restart involves only a process restart and if it is non reload- no change in process takes place.

Step 5 Select the SMU and click on **Activate** to activate the SMU on the system and install the package, and update the package status details.

Step 6 Select the SMU and click **Commit** to make the activation changes persistent across reloads.

The Commit operation creates commit points. These commit points are similar to snapshots using which you can determine which specific change you want to be activated or rolled back to, in case there is any issue with

the SMU. The commit can be done after activation when the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload.

Installing SMU

Procedure

	Command or Action	Purpose
Step 1	**install add file bootflash:** *filename* **Example:** `Device# install add file bootflash:<Filename>`	Copies the maintenance update package from a remote location to the device, and performs a compatibility check for the platform and image versions. This command runs base compatibility checks on a file to ensure that the SMU package is supported on the platform. It also adds an entry in the package/SMU.sta file, so that its status can be monitored and maintained.
Step 2	**install activate file bootflash:** *filename* **Example:** `Device# install activate file bootflash:<Filename>`	Runs compatibility checks, installs the package, and updates the package status details. For a restartable package, the command triggers the appropriate post-install scripts to restart the necessary processes, and for non-restartable packages it triggers a reload.
Step 3	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads. The commit can be done after activation while the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload, but not after the second reload.
Step 4	**show version** **Example:** `Device# show version`	Displays the image version on the device.
Step 5	**show install summary** **Example:** `Device# show install summary`	Displays information about the active package. The output of this command varies according to the install commands that are configured.

Roll Back an Image (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management**.
Step 2 Go to **SMU**, **APSP** or **APDP**.
Step 3 Click **Rollback**.
Step 4 In the **Rollback to** drop-down list, choose **Base**, **Committed** or **Rollback Point**.
Step 5 Click **Add File**.

Rollback SMU

Procedure

	Command or Action	Purpose
Step 1	**install rollback to** {**base** | **committed** | **id** | **committed** } *committed ID* **Example:** `Device(config)# install rollback to id 1234`	Returns the device to the previous installation state. After the rollback, a reload is required.
Step 2	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads.

Deactivate SMU

Procedure

	Command or Action	Purpose
Step 1	**install deactivate file bootflash:** *filename* **Example:** `Device# install deactivate file bootflash:<Filename>`	Deactivates an active package, updates the package status, and triggers a process to restart or reload.
Step 2	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads.

Configuration Examples for SMU

The following is sample of the SMU configuration, after the install add for the SMU is done:

```
Device#show install summary

[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------

IMG   C    16.8.1.0.39751

--------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------
```

Information About AP Device Package

The controller supports rolling out critical bug fixes using Software Maintenance Upgrade (SMU). Similarly, if any new AP hardware model is introduced, the AP models need to be connected to the existing wireless network.

Currently, when a new AP hardware model is introduced, those get shipped along with the corresponding controller related major software version. Then you need to wait for the release of a corresponding controller version relative to the new AP model and upgrade the entire network.

From 16.11.1 onwards, you can introduce the new AP model into your wireless network using the SMU infrastructure without the need to upgrade to the new controller version. This solution is termed as AP Device Package (APDP).

SMU Process or Workflow

The SMU process builds APDP to detect code changes and build APDP. It also supports addition of a new file (AP image file) to APDP and inclusion of those AP images into APDP.

The workflow is as follows:

- install add
- install activate
- install commit

For more details, see *Managing AP Device Package*.

Note To ensure completion of the APSP or APDP activation or deactivation process, ensure that you run the **install commit** command after the **install activate** or **install deactivate** command. Failing to do so within 6 hours of the deactivate operation terminates the deactivate operation and moves it back to the original commit position.

SMU Package

A SMU package contains the metadata that carry AP model and its capability related details.

AP Image Changes

When new AP models are introduced, there may or may not be corresponding new AP images. This means that AP images are mapped to the AP model families. If a new AP model belongs to an existing AP model family then you will have existing AP image entries (Example: ap3g3, ap1g5, and so on). For instance, if an AP model belongs to either ap3g3 or ap1g5, the respective image file is updated with the right AP image location. Also, the corresponding metadata file is updated with the new AP model capability information.

If a new AP model belongs to a new AP model family and new image file, the new image entry file is created in the right AP image location. Also, the corresponding metadata file is updated with the new AP model capability information.

During AP image bundling and packaging of APDP, the new AP model images and metadata file are packaged into APDP.

Note The APDP images must not be renamed to avoid impact on its functionality.

Installing AP Device Package (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management**.

Step 2 Click **AP Device Package (APDP)** tab.

Step 3 Click **Add**.

Step 4 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as TFTP, SFTP, FTP, Device, or Desktop (HTTP).

a) If you choose **TFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose a **File System** from the drop-down list.

b) If you choose **SFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and choose a **File System** from the drop-down list.

c) If you choose **FTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and choose a **File System** from the drop-down list.

d) If you choose **Device** as the **Transport Type**, you need to enter the **File path** and choose a **File System** from the drop-down list.

e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose a **File System** from the drop-down list and click **Select File** to navigate to the **Source File Path**.

Step 5 Enter the **File Name** and click **Add File**.

Step 6 From the **AP Upgrade Configuration** section, choose the percentage of APs to be included from the **AP Upgrade per iteration** drop-down list.

Step 7 Click **Apply**.

Installing AP Device Package (CLI)

Procedure

	Command or Action	Purpose
Step 1	**install add file bootflash:** *filename* **Example:** `Device# install add file bootflash:<Filename>`	Extracts AP images from APDP and places them in SMU or APDP specific mount location. **Note** Here, the SMU does not trigger the Wireless module.
Step 2	**install activate file bootflash:** *filename* **Example:** `Device# install activate file bootflash:<Filename>`	Adds the AP software in APDP to the existing current active AP image list. Also, updates the capability information for the new AP models in the controller . **Note** Even if the new AP module supports new hardware capabilities, the controller recognizes only the capability information that its base version supports. At this point, the controller accepts the new connection from the new AP model. The new AP model then joins the controller .
Step 3	**install commit** **Example:** `Device# install commit`	Commits the new AP software to be persistent across reloads. The commit can be done after activation while the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload, but not after the second reload.
Step 4	**install deactivate file bootflash:** *filename* **Example:** `Device# install deactivate file bootflash:<Filename>`	(Optional) Deactivates an active APDP, updates the package status, and triggers a process to restart or reload.
Step 5	**show version** **Example:** `Device# show version`	Displays the image version on the device.

Verifying APDP on the Controller

To verify the status of APDP packages on the controller , use the following command:

```
Device# show install summary

[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
APDP  I    bootflash:apdp_CSCvp12345.bin
IMG   C    17.1.0.0
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Note The output of this command varies based on the packages, and the package states that are installed.

Information About Per Site or Per AP Model Service Pack (APSP)

The controller supports critical updates to the access points (APs) using Software Maintenance Update (SMU). Using the Per Site or Per AP Model Service Pack feature, you can roll out critical AP bug fixes to a subset of APs, on a site or group of sites, using SMU in a staggered manner.

This feature allows to control the propagation of a SMU in your network by selecting the sites, to be included in the SMU activation, using Per Site AP SMU rollout. However, all sites should be brought to the same SMU level before a new SMU can be rolled out to a subset of sites or for a subsequent image upgrade to be initiated on the system..

Using Per AP model SMU, you can limit the update to only certain AP models. The software is predownloaded and is activated only to certain AP models, within a site. Note that if a certain number of model images are included in a SMU, all the future updates must contain software images for those models.

This feature is supported in the flex-connect mode, local mode, and Software-Defined Access (SD-Access) wireless scenarios.

Note After applying the AP site filter for per site SMU upgrade, a new image installation will not be allowed without applying the site filter to all the other sites, or removing the existing site filter.

Restrictions

- If APs are not configured to a primary controller, the APs will see the same discovery response from controllers with the APSP image and without the APSP image, causing the APs to flap between two controllers.

Workflow of AP SMU Upgrade

- Run a query to check whether there are ongoing activities, such as AP image predownload or AP rolling upgrade.
- Identify the site or sites to install the SMU in, and set up a site filter.

- Trigger the predownload of SMU to the sites in the site filter.
- Activate the SMU after the predownload is complete.
- Commit the update.

Note You can add more sites to a filter after setting up the filter. However, you have to apply the filter again using the **ap image site-filter file** *file-name* **apply** command. If you clear the site filter, the update is made on all the remaining sites. Deactivation and rollback of the images are not filtered per site, and are applicable to all the sites.

Rolling AP Upgrade

Rolling AP upgrade is a method of upgrading the APs in a staggered manner such that some APs are always up in the network and provide seamless coverage to clients, while the other APs are selected to be upgraded.

Note The AP images should be downloaded before the rolling upgrade is triggered, so that all the APs that are to be upgraded have the new image version.

Note The time required to complete Rolling AP upgrade depends on factors such as the number of APs, the percentage of APs in each iteration, the controller type, and the connectivity between the controller and the APs. In general, Rolling AP upgrade completion time is the max iteration time (where each iteration can take up to 5 minutes) * expected number of iterations. You use the *iteration expiry time* field of the **show ap upgrade** command output to see the end time.

Rolling AP Upgrade Process

Rolling AP upgrade is done on a per controller basis. The number of APs to be upgraded at a given time, is the percentage of the total number of APs that are connected to the controller. The percentage is capped at a user configured value. The default percentage is 15. The non-client APs will be upgraded before the actual upgrade of APs begin.

The upgrade process is as follows:

1. **Candidate AP Set Selection**

   In this stage, a set of AP candidates are selected based on neighboring AP information. For example, if you identify an AP for upgrade, a certain number (N) of its neighbors are excluded from candidate selection. The N values are generated in the following manner:

   If the user configurable capped percentage is 25%, then N=6 (Expected number of iterations =5)

   If the user configurable capped percentage is 15%, then N=12 (Expected number of iterations=12)

   If the user configurable capped percentage is 5%, then N=24 (Expected number of iterations =22)

If the candidates cannot be selected using the neighboring AP information, select candidates from indirect neighbors. If you still are not able to select candidates, the AP will be upgraded successfully without any failure.

Note After the candidates are selected, if the number of candidates are more than the configured percentage value, the extra candidates are removed to maintain the percentage cap.

2. **Client Steering**

   Clients that are connected to the candidate APs are steered to APs that are not there in the candidate AP list, prior to rebooting the candidate APs. The AP sends out a request to each of its associated clients with a list of APs that are best suited for them. This does not include the candidate APs. The candidate APs are marked as unavailable for neighbor lists. Later, the markings are reset in the AP rejoin and reload process.

3. **AP Rejoin and Reload Process**

   After the client steering process, if the clients are still connected to the candidate AP, the clients are sent a de-authorization and the AP is reloaded and comes up with a new image. A three-minute timer is set for the APs to rejoin. When this timer expires, all the candidates are checked and marked if they have either joined the controller or the mobility peer. If 90% of the candidate APs have joined, the iteration is concluded; if not, the timer is extended to three more minutes. The same check is repeated after three minutes. After checking thrice, the iteration ends and the next iteration begins. Each iteration may last for about 10 minutes.

   For rolling AP upgrade, there is only one configuration that is required. It is the number of APs to be upgraded at a time, as a percentage of the total number of APs in the network.

   Default value will be 15.

```
Device (config)#ap upgrade staggered <25 | 15 | 5>
```

Use the following command to trigger the rolling AP upgrade:

```
Device#ap image upgrade [test]
```

Note Rolling AP upgrade is not resumed after an SSO. You should run the **ap image upgrade** command to restart the rolling AP upgrade from the beginning and it affects all the APs, including the Mesh APs.

Installing AP Service Package (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management**.

Step 2 Click **AP Service Package (APSP)** tab.

Step 3 Click **Add**.

Step 4 From the **Transport Type** drop-down list, choose the transfer type to transfer the software image to your device as TFTP, SFTP, FTP, Device, or Desktop (HTTP).

a) If you choose **TFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **File path** and choose a **File System** from the drop-down list.
b) If you choose **SFTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **SFTP Username**, **SFTP Password**, **File path** and choose a **File System** from the drop-down list.
c) If you choose **FTP** as the **Transport Type**, you need to enter the **Server IP Address (IPv4/IPv6)**, **FTP Username**, **FTP Password**, **File path**, and choose a **File System** from the drop-down list.
d) If you choose **Device** as the **Transport Type**, you need to enter the **File path** and choose a **File System** from the drop-down list.
e) If you choose **Desktop (HTTPS)** as the **Transport Type**, you need to choose a **File System** from the drop-down list and click **Select File** to navigate to the **Source File Path**.

Step 5 Enter the **File Name** and click **Add File**.

Step 6 From the **AP Upgrade Configuration** section, choose the percentage of APs to be included from the **AP Upgrade per iteration** drop-down list.

Step 7 Click **Apply**.

Installing AP Service Package (CLI)

Use the following procedure to roll out critical bug fixes to a subset of APs using SMU.

Procedure

	Command or Action	Purpose
Step 1	**install add file** *file-name* **Example:** `Device# install add file flash:<file-name>`	Checks for ongoing activities, such as AP image predownload or AP rolling upgrade. If there are no such activities, populates the predownload directory to install a package file to the system.
Step 2	**ap image site-filter file** *file-name* **add** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> add bgl18`	Adds a site tag to a site filter.
Step 3	**ap image site-filter file** *file-name* **remove** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> remove bgl18`	(Optional) Removes a site tag from a site filter.
Step 4	**ap image predownload** **Example:** `Device# ap image predownload`	(Optional) Performs predownload of an AP image. This image predownload will be filtered by the site filter, set up in the previous step.
Step 5	**install activate file** *file-name* **Example:**	Triggers the AP upgrade in rolling a staggered fashion for the APs added in site filter.

	Command or Action	Purpose
	`Device# install activate file flash:<file-name>`	
Step 6	**install commit** **Example:** `Device# install commit`	Commits the image update. During the commit, the mapping from file to site is saved in the persistent database so that it is available even after a reload.

Adding a Site to a Filter

Procedure

	Command or Action	Purpose
Step 1	**ap image site-filter file** *file-name* **add** *site-tag* **Example:** `Device# ap image site-filter file flash:<file-name> add bgl18`	Adds a site tag to a site filter. Repeat this step again to set up a multisite filter.
Step 2	**ap image site-filter file** *file-name* **apply** **Example:** `Device# ap image site-filter file flash:<file-name> apply`	Predownloads the image and upgrades the APs based on the site filter.
Step 3	**ap image site-filter file** *file-name* **clear** **Example:** `Device# ap image site-filter file flash:<file-name> clear`	Clears the site filter table and predownloads the image and does a rolling AP upgrade to all sites where it is not active.

Deactivating an Image

Procedure

	Command or Action	Purpose
Step 1	**install deactivate file flash** *file-name* **Example:** `Device# install deactivate file flash:<file-name>`	Performs rolling AP upgrade based on the AP models present in the prepare file. Deactivation is not filtered by site. Therefore, deactivation applies to all the sites. **Note** Action is taken if the APs in a site are not running the SMU that is being deactivated. Only internal tables are updated to remove the SMU.

Roll Back APSP

Procedure

	Command or Action	Purpose
Step 1	**install add profile** *rollback_profile-name* **Example:** `Device# install add profile rollback_id1`	(Optional) Moves back to any rollback points in a graceful way with AP image predownload support. **Note** To get a list of available rollback profile names, use **show install profile** command.
Step 2	**ap image predownload** **Example:** `Device# ap image predownload`	(Optional) Performs predownload of an AP image. This image predownload will be filtered by the site filter, set up in the previous step.
Step 3	**install rollback to** *rollback_id* **Example:** `Device# install rollback to rollback_id1`	Performs rollback of the image for the affected AP models. The roll back action is not filtered by site. Therefore, rollback applies to all the sites. **Note** The APs that are in the base image or in a point before the rollback action takes effect are not affected.

Canceling the Upgrade

Procedure

	Command or Action	Purpose
Step 1	**install abort** **Example:** `Device# install abort`	Aborts the upgrade by resetting the APs in rolling fashion.

Verifying the Upgrade

To see the summary of the AP software install files, use the following command:

```
Device# show ap image file summary

AP Image Active List
============================
Install File Name: base_image.bin
------------------------------
AP Image Type    Capwap Version  Size (KB)         Supported AP models
```

```
-------------    --------------
---------------------------------------------------------------------
     ap1g1       17.3.0.30        13300   NA

     ap1g2       17.3.0.30        34324   NA

     ap1g3       17.3.0.30        98549   AP803

    ap1g4       17.3.0.30             34324   AP1852E, AP1852I, AP1832I, AP1830I, AP1810W,
 OEAP1810

    ap1g5      17.3.0.30            23492   AP1815W, AP1815T, OEAP1815, AP1815I, AP1800I,
 AP1800S, AP1815M, 1542D, AP1542I, AP1100AC, AP1101AC, AP1840I

     ap1g6       17.3.0.30        93472               AP2900I, C9117AXI

   ap1g6a       17.3.0.30       247377             C9130AXI, C9130AXE, C9140AXI, C9140AXD,
 C9140AXT

     ap1g7       17.3.0.30        23988               AP1900I, C9115AXI, AP1900E, C9115AXE,
 C9120AXE, C9120AXP, C9120AXI

     ap1g8       17.3.0.30        23473   C9105AXI, C9105AXW, C9110AXI, C9110AXE

     ap3g1       17.3.0.30        23422   NA

     ap3g2       17.3.0.30        23411   AP1702I

     ap3g3       17.3.0.30        23090   AP3802E, AP3802I, AP3802P, AP4800, AP2802E,
AP2802I, AP2802H, AP3800, AP1562E, AP1562I, AP1562D, AP1562PS, IW-6300H-DC, IW-6300H-AC,
IW-6300H-DCW, ESW-6300

     c1570       17.3.0.30        13000   AP1572E, 1573E, AP1572I

     c3700       17.3.0.30        14032   AP3702E, AP3701E, AP3701I, AP3702I, AP3701P,
AP3702P, AP2702E, AP2702I, AP3702, IW3702, AP3701, AP3700C

 virtApImg       17.3.0.30                   177056        APVIRTUAL


AP Image Prepare List**
============================
Install File Name: base_image.bin
------------------------------
============================
Install File Name: base_image.bin
------------------------------
AP Image Type    Capwap Version  Size (KB)         Supported AP models
-------------    --------------
---------------------------------------------------------------------
     ap1g1       17.3.0.30     13300             NA

     ap1g2       17.3.0.30     34324             NA

     ap1g3       17.3.0.30     98549             AP803

     ap1g4       17.3.0.30           34324             AP1852E, AP1852I, AP1832I, AP1830I,
 AP1810W, OEAP1810

     ap1g5       17.3.0.30          23492             AP1815W, AP1815T, OEAP1815, AP1815I,
 AP1800I, AP1800S, AP1815M, 1542D, AP1542I, AP1100AC, AP1101AC, AP1840I

     ap1g6       17.3.0.30     93472                         AP2900I, C9117AXI
```

```
   ap1g6a       17.3.0.30     247377                        C9130AXI, C9130AXE, C9140AXI,
C9140AXD, C9140AXT

    ap1g7       17.3.0.30     23988                  AP1900I, C9115AXI, AP1900E, C9115AXE,
C9120AXE, C9120AXP, C9120AXI

    ap1g8       17.3.0.30     23473             C9105AXI, C9105AXW, C9110AXI, C9110AXE

    ap3g1       17.3.0.30     23422             NA

    ap3g2       17.3.0.30     23411             AP1702I

    ap3g3       17.3.0.30     23090            AP3802E, AP3802I, AP3802P, AP4800, AP2802E,
AP2802I, AP2802H, AP3800, AP1562E, AP1562I, AP1562D, AP1562PS, IW-6300H-DC, IW-6300H-AC,
IW-6300H-DCW, ESW-6300

    c1570       17.3.0.30     13000             AP1572E, 1573E, AP1572I

   c3700       17.3.0.30     14032            AP3702E, AP3701E, AP3701I, AP3702I, AP3701P,
AP3702P, AP2702E, AP2702I, AP3702, IW3702, AP3701, AP3700C

virtApImg       17.3.0.30                 177056            APVIRTUAL

**Difference of Active and Prepare list gives images being predownloaded to Access Points.
```

To see the summary of the AP site-filtered upgrades, use the following command:

```
Device# show ap image site summary

Install File Name: vwlc_apsp_16.11.1.0_74.bin

Site Tag                                  Prepared         Activated        Committed

-------------------------------------------------------------------------------------------
bgl-18-1                                  Yes              Yes              Yes

bgl-18-2                                  Yes              Yes              Yes

bgl-18-3                                  Yes              Yes              Yes

default-site-tag                          Yes              Yes              Yes
```

To see the summary of AP upgrades, use the following command:

```
Device# show ap upgrade summary
```

To check the status of an APSP, use the following command:

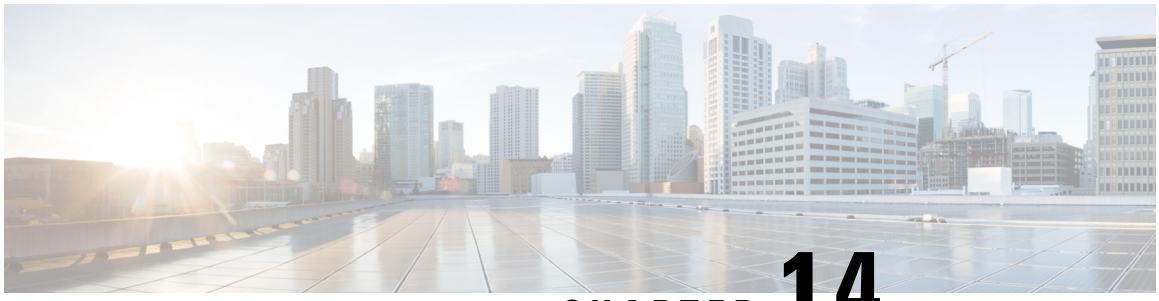
```
Device# show install summary

[ Chassis 1 ] Installed Package(s) Information:

State (St): I - Inactive, U - Activated & Uncommitted,

C - Activated & Committed, D - Deactivated & Uncommitted

--------------------------------------------------------------------------------

Type St Filename/Version

--------------------------------------------------------------------------------

APSP I bootflash:vwlc_apsp_16.11.1.0_74.bin
```

```
IMG C 16.11.1.0.1249


--------------------------------------------------------------------------------

Auto abort timer: inactive

--------------------------------------------------------------------------------
```

Verifying of AP Upgrade on the Controller

Use the following **show** command to verify the AP upgrade on the controller:

```
Device #show ap upgrade

AP upgrade is in progress
From version: 8 16.9.1.6
To version: 9 16.9.1.30
Started at: 03/09/2018 21:33:37 IST
Percentage complete: 0
Expected time of completion: 03/09/2018 22:33:37 IST
Progress Report
---------------
Iterations
----------
Iteration Start time End time AP count
-------------------------------------------------------------------------
0 03/09/2018 21:33:37 IST 03/09/2018 21:33:37 IST 0
1 03/09/2018 21:33:37 IST ONGOING 0
Upgraded
--------
Number of APs: 0
AP Name Ethernet MAC Iteration Status
-------------------------------------------------------------------------
In Progress
-----------
Number of APs: 1
AP Name Ethernet MAC
-------------------------------------------------
APf07f.06a5.d78c f07f.06cf.b910
Remaining
---------
Number of APs: 3
AP Name Ethernet MAC
-------------------------------------------------
APCC16.7EDB.6FA6 0081.c458.ab30
AP38ED.18CA.2FD0 38ed.18cb.25a0
AP881d.fce7.5ee4 d46d.50ee.33a0
```



CHAPTER 14

Efficient Image Upgrade

- Efficient Image Upgrade, on page 241
- Enable Pre-Download (GUI), on page 241
- Enable Pre-Download (CLI), on page 242
- Configuring a Site Tag (CLI), on page 242
- Attaching Policy Tag and Site Tag to an AP (CLI), on page 243
- Trigger Predownload to a Site Tag, on page 244

Efficient Image Upgrade

Efficient Image upgrade is an optimized method of predownloading images to FlexConnect APs. For each Site Tag with FlexConnect APs joined, one AP per model in that Site Tag is selected as the primary AP, and downloads its image from the controller through the WAN link. Once the primary AP has the downloaded image, the APs in that Site Tag start downloading the image from the primary AP, via TFTP. At most three subordinate APs can download simultaneously from the primary. This reduces load on the WAN link.

Note Make sure that all APs joined via a Site Tag are at the same location, before enabling this feature.

Enable Pre-Download (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Access Points** page, expand the **All Access Points** section and click the name of the AP to edit.

Step 3 In the **Edit AP** page, click the **Advanced** tab and from the **AP Image Management** section, click **Predownload**.

Step 4 Click **Update & Apply to Device**.

Enable Pre-Download (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a flex profile and enters the flex profile configuration mode.
Step 3	**predownload** **Example:** `Device(config-wireless-flex-profile)# predownload`	Enables predownload of the image.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits the configuration mode and returns to privileged EXEC mode.

Configuring a Site Tag (CLI)

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site rr-xyz-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:**	Configures a flex profile.

	Command or Action	Purpose
	`Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	**Note** You cannot remove the flex profile configuration from a site tag if local site is configured on the site tag. **Note** The **no local-site** command needs to be used to configure the Site Tag as Flexconnect, otherwise the Flex profile config does not take effect.
Step 4	**description** *site-tag-name* **Example:** `Device(config-site-tag)# description "default site tag"`	Adds a description for the site tag.
Step 5	**end** **Example:** `Device(config-site-tag)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless tag site summary** **Example:** `Device# show wireless tag site summary`	(Optional) Displays the number of site tags. **Note** To view detailed information about a site, use the **show wireless tag site detailed** *site-tag-name* command. **Note** The output of the **show wireless loadbalance tag affinity wncd** *wncd-instance-number* command displays default tag (site-tag) type, if both site tag and policy tag are not configured.

Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures a Cisco AP and enters AP profile configuration mode. **Note** The *mac-address* should be a wired mac address.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag rr-xyz-site`	Maps a site tag to the AP.
Step 5	**rf-tag** *rf-tag-name* **Example:** `Device(config-ap-tag)# rf-tag rf-tag1`	Associates the RF tag.
Step 6	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 7	**show ap tag summary** **Example:** `Device# show ap tag summary`	(Optional) Displays AP details and the tags associated to it.
Step 8	**show ap name** <*ap-name*> **tag info** **Example:** `Device# show ap name ap-name tag info`	(Optional) Displays the AP name with tag information.
Step 9	**show ap name** <*ap-name*> **tag detail** **Example:** `Device# show ap name ap-name tag detail`	(Optional) Displays the AP name with tag details.

Trigger Predownload to a Site Tag

Follow the procedure given below to trigger image download to the APs:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> configure terminal`	Enters the privileged EXEC mode.
Step 2	**ap image predownload site-tag** *site-tag* **start** **Example:** `Device# ap image predownload site-tag rr-xyz-site start`	Instructs the primary APs to start image predownload.
Step 3	**show ap master list** **Example:** `Device# show ap master list`	Displays the list of primary APs per AP model per site tag.
Step 4	**show ap image** **Example:** `Device# show ap image`	Displays the predownloading state of primary and subordinate APs . **Note** To check if Flexefficient image upgrade is enabled in the AP, use the **show capwap client rcb** command on the AP console.

The following sample outputs display the functioning of the Efficient Image Upgrade feature:

The following output displays the primary AP.

```
Device# show ap master list
AP Name                          WTP Mac          AP Model          Site Tag
-------------------------------------------------------------------------------------
AP0896.AD9D.3124                 f80b.cb20.2460   AIR-AP2802I-D-K9 ST1
```

The following output shows that the primary AP has started predownloading the image.

```
Device# show ap image
Total number of APs: 6

AP Name             Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
-------------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     0.0.0.0       None                 0.0.0.0
  N/A               0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
  N/A               0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
  N/A               0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
  N/A               0
AP0896.AD9D.3124    16.6.230.37     8.4.100.0     Predownloading       16.6.230.36
  0                 0
AP2C33.1185.C4D0    16.6.230.37     8.4.100.0     None                 0.0.0.0
  N/A               0
```

The following output shows that the primary AP has completed predownload and the predownload has been initiated in the subordinate AP.

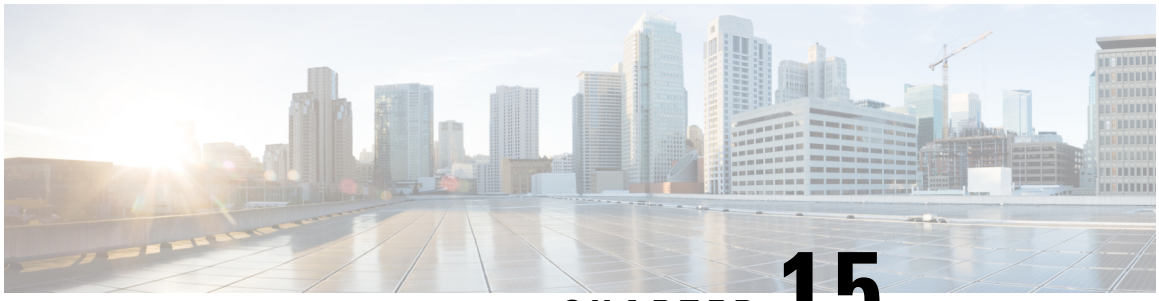
```
Device# show ap image

Total number of APs: 6
AP Name             Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
------------------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     0.0.0.0       Initiated            16.6.230.36
  N/A               0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
  N/A               0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
  N/A               0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
  N/A               0
AP0896.AD9D.3124    16.6.230.37     8.4.100.0     Complete             16.6.230.36
  0                 0
AP2C33.1185.C4D0    16.6.230.37     8.4.100.0     Initiated            16.6.230.36
  0                 0
```

The following output shows image status of a particular AP.

```
Device# show ap name APe4aa.5dd1.99b0 image
AP Name : APe4aa.5dd1.99b0
Primary Image : 16.6.230.46
Backup Image : 3.0.51.0
Predownload Status : None
Predownload Version : 000.000.000.000
Next Retry Time : N/A
Retry Count : 0
```

The following output shows predownload completion on all APs.

```
Device# show ap image
Total number of APs: 6

Number of APs
        Initiated                 : 0
        Predownloading            : 0
        Completed predownloading  : 3
        Not Supported             : 0
        Failed to Predownload     : 0

AP Name             Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
------------------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     16.6.230.36   Complete             16.6.230.36
  N/A               0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
  N/A               0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
  N/A               0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
  N/A               0
AP0896.AD9D.3124    16.6.230.37     16.6.230.36   Complete             16.6.230.36
  0                 0
AP2C33.1185.C4D0    16.6.230.37     16.6.230.36   Complete             16.6.230.36
  0                 0
```



CHAPTER 15

Predownloading an Image to an Access Point

- Information About Predownloading an Image to an Access Point, on page 247
- Restrictions for Predownloading an Image to an Access Point, on page 247
- Predownloading an Image to Access Points (CLI), on page 248
- Predownloading an Image to Access Points (GUI), on page 250
- Predownloading an Image to Access Points (YANG), on page 250
- Monitoring the Access Point Predownload Process, on page 251
- Information About AP Image Download Time Enhancement (OEAP or Teleworker Only), on page 252
- Configuring AP Image Download Time Enhancement (GUI), on page 253
- Configuring AP Image Download Time Enhancement (CLI), on page 253
- Verifying AP Image Download Time Enhancement Configuration, on page 254

Information About Predownloading an Image to an Access Point

To minimize network outages, download an upgrade image to an access point from the device without resetting the access point or losing network connectivity. Previously, you could download an upgrade image to the device and reset it, causing the access point to go into discovery mode. After the access point discovered the controller with the new image, the access point would download the new image, reset it, go into discovery mode, and rejoin the device.

You can now download the upgrade image to the controller. When the controller is up with the upgrade image, the AP joins the controller and moves to Registered state, because the AP image has been predownloaded to the AP.

Restrictions for Predownloading an Image to an Access Point

The following are the restrictions for predownloading an image to an access point:

- The maximum number of concurrent predownloads are limited to 100 per wncd instance (25 for 9800-L) in the controller. However, the predownloads are triggered in sets of 16 per wncd instance at the start, and is repeated every 60 seconds.
- Access points with 16-MB total available memory may not have enough free memory to download an upgrade image and may automatically delete crash information files, radio files, and backup images, if any, to free up space. However, this limitation does not affect the predownload process because the predownload image replaces backup image, if any, on the access point.

- All of the primary, secondary, and tertiary controllers should run the same images. Otherwise, the feature will not be effective.
- At the time of reset, you must make sure that all of the access points have downloaded the image.
- An access point can store only 2 software images.
- The Cisco Wave 1 APs may download the image twice while moving from Cisco AireOS Release 8.3 to Cisco IOS XE Gibraltar 16.10.1. This increases the AP downtime during migration.
- The **show ap image** command displays cumulative statistics regarding the AP images in the controller. We recommend that you clear the statistics using the **clear ap predownload statistics** command, before using the show ap image command, to ensure that correct data is displayed.
- Cisco Catalyst 9800-CL Wireless Controller supports only self-signed certificates and does not support Cisco certificates. When you move the access points between Cisco Catalyst 9800-CL Wireless Controllers, and if the AP join failure occurs on the Cisco Catalyst 9800-CL controller, execute the **capwap ap erase all** command to remove the hash string stored on the APs.
- During AP image pre-download, the WNCD CPU may rise to 99 percent, which is normal and doesn't cause a crash or client or AP disconnect problems.

Predownloading an Image to Access Points (CLI)

Before you begin

There are some prerequisites that you must keep in mind while predownloading an image to an access point:

- Predownloading can be done only when the device is booted in the install mode.

Note Predownload of the AP image is based on the AP model rather than the image type. Predownload is allowed only when the model exists in the new capability XML file. Also, with appropriate modification of the capability XML, the controller can override the existing AP image for a particular model.

- You can copy the new image either from the TFTP server, flash image, or USB.
- If the latest upgrade image is already present in the AP, predownload will not be triggered. Check whether the primary and backup image versions are the same as the upgrade image, using the **show ap image** command.
- The **show ap image** command displays cumulative statistics regarding the AP images in the controller. We recommend that you clear the statistics using the **clear ap predownload statistics** command, before using the **show ap image** command, to ensure that correct data is displayed.
- AP continues to be in predownloading state, if AP flaps post SSO during AP predownload. We recommended that you issue the **ap image predownload abort** command and then the **clear ap predownload stats** command only then the predownload can be intiated again.

Procedure

	Command or Action	Purpose
Step 1	**install add file bootflash:***file-name* **Example:** `Device# install add file bootflash:image.bin`	The controller software image is added to the flash and expanded.

Step 2	**ap image predownload** or **ap name** *ap-name* **image predownload**
	Example:
	`Device# ap image predownload`
	`Device# ap name ap1 image predownload`
		Downloads the new image to all the access points or a specific access point connected to the device.

Step 3	**show ap image** **Example:** `Device# show ap image`	Verifies the access point's predownload status. This command initially displays the status as Predownloading and then moves to Completed, when download is complete.
Step 4	**show ap name** *ap-name* **image** **Example:** `Device# show ap name ap1 image`	Provides image details of a particular AP.
Step 5	**ap image swap** `or`**ap name** *ap-name* **image swap** `or`**ap image swap completed** **Example:** `Device# ap image swap`	Swaps the images of the APs that have completed predownload. **Note** You can swap the AP images using **ap image swap** command even without pre-downloading a new image to the AP and there are no restrictions or prerequisites to swap the image.
Step 6	**install activate** **Example:** `Device# install activate`	Runs compatibility checks, installs the package, and updates the package status details. For a restartable package, the command triggers the appropriate post-install scripts to restart the necessary processes, and for non-restartable packages it triggers a reload. **Note** This step reloads the complete controller stack (both primary and secondary controllers, if HA is used).
Step 7	**install commit** **Example:** `Device# install commit`	Commits the activation changes to be persistent across reloads. The commit can be done after activation while the system is up, or after the first reload. If the

	Command or Action	Purpose
		package is activated but not committed, it remains active after the first reload, but not after the second reload.

Predownloading an Image to Access Points (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management** and click the **Software Upgrade** tab.

Note that you must be in the Install Mode to continue with the following steps.

Step 2 Select the **Transport Type, File System and File Path** of your choice to from receive the file.

Step 3 Select the **AP Image Predownload** check box.

If you already have an inactive image file on your device, a dialog box prompts you to remove the unused image and proceed with the latest image download.

Step 4 Click **Download & Install**.

This initiates the upgrade process and you can view and verify the predownload progress in the **Status** dialog box. You can also check the progress log by clicking on **Show Logs** icon.

Step 5 Click the **Save Configuration & Activate** button after the predownload operation is successful.

Step 6 Click **Yes** to confirm the activate operation.

This operation runs compatibility checks, installs the package, and updates the package status details. The device reloads after a successful activation. If there are uncommitted files, you are prompted to remove those.

Step 7 Click the **Commit** button to complete the upgrade process.

Predownloading an Image to Access Points (YANG)

YANG can be used with NETCONF and RESTCONF to provide the desired solution of automated and programmable network operations.

The following RPC is used for Predownloading an Image to an Access Point:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <set-rad-predownload-all
xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-cmd-rpc">
    <uuid>12312341231234</uuid>
  </set-rad-predownload-all>
</rpc>
```

For more information on the YANG models, see the Cisco IOS XE Programmability Configuration Guide and YANG Data Models on Github at https://github.com/YangModels/yang/tree/master/vendor/cisco/xe.

You can contact the Developer Support Community for NETCONF/YANG features using the following link:

https://developer.cisco.com/

Monitoring the Access Point Predownload Process

This section describes the commands that you can use to monitor the access point predownload process.

While downloading an access point predownload image, enter the **show ap image** command to verify the predownload progress on the corresponding access point:

```
Device# show ap image
Total number of APs  : 1

Number of APs
       Initiated                : 1
       Predownloading           : 1
       Completed predownloading   : 0
       Not Supported            : 0
       Failed to Predownload      : 0

AP Name                         Primary Image   Backup Image    Predownload Status
Predownload Ver...  Next Retry Time    Retry Count
-------------------------------------------------------------------------------------
AP1                             10.0.1.66       10.0.1.66       Predownloading
10.0.1.67           NA                          0


Device# show ap image

Total number of APs  : 1

Number of APs
       Initiated                : 1
       Predownloading           : 0
       Completed predownloading   : 1
       Not Supported            : 0
       Failed to Predownload      : 0

AP Name                         Primary Image   Backup Image    Predownload Status
Predownload Ver...  Next Retry Time    Retry Count
-------------------------------------------------------------------------------------
AP1                             10.0.1.66       10.0.1.67       Complete
10.0.1.67           NA
                        0
```

Use the following command to view the image details of a particular AP:

```
Device# show ap name APe4aa.5dd1.99b0 image

AP Name : APe4aa.5dd1.99b0
Primary Image : 16.6.230.46
Backup Image : 3.0.51.0
Predownload Status : None
Predownload Version : 000.000.000.000
Next Retry Time : N/A
Retry Count : 0
```

Information About AP Image Download Time Enhancement (OEAP or Teleworker Only)

The wireless controller and the access point (AP) communicate with each other using CAPWAP. The CAPWAP has two channels, namely control and data. The control channel is used to send configuration messages, download images and client keys, or the context to the AP. The control channel has a single window in the current implementation. A single window means that every message that is sent from the controller has to be acknowledged by the AP. The next control packet is not transmitted till the earlier one is acknowledged by the AP.

The AP Image Download Time Enhancement feature adds support to multiple sliding windows for control packets going from controller to AP. The sliding window can be set to N (static) instead of a single window. The request queue size is decided based on the maximum window size the AP supports.

Table 16: Recommended Window Size

Link Bandwidth[6]	Less than 200 ms RTT	Greater than 200 ms RTT
More than 20 Mbps	10	15
Between 5 and 20 Mbps	10	15
Between 1 and 5 Mbps	5	10
Less than 1 Mbps	3	5

[6] The window size recommendation provided in the table is for packet loss of less than one percent (< 1%). If the network supporting the CAPWAP link has packet loss of more than one percent (> 1%), use a smaller value for window size. For good links with round-trip time (RTT) of about 100ms and packet drops of less than half a percent (< 0.5%), use a window size of up to 20 for better performance.

Note

- The window size can be changed only during the AP join process.
- All image upgrades should be in the **install** mode for faster upgrade. Image upgrade should be done from the **one-shot** command to include OEAP predownload.
- Configure the window size only for AP profiles that are exclusively used for Teleworker or Office Extend Access Points (OEAP).
- An AP reload is not required after disabling this feature.
- This feature is supported only on the OEAP profiles.
- GUI does not support AP predownload. Therefore, the AP downloads after disjoining the controller during CAPWAP join phase. This causes a long disruption in the network as the Image download for AP can take upto one hour.

Important If you downgrade the software to Cisco IOS XE Gibraltar 16.12.4 or earlier from Cisco IOS XE Amsterdam 17.3.1, you should reset the CAPWAP multi window to a single window prior to the downgrade. Failure to do so necessitates a manual AP recovery.

High-Level Workflow of AP Image Download Time Enhancement

1. Select an existing AP join profile or create a new one.
2. Set the CAPWAP window size.
3. Associate the AP join profile to an existing site tag or new one.
4. Apply the site tag to the AP using: Static, Filter, Location, AP, or Default mapping method.

Configuring AP Image Download Time Enhancement (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join** > **CAPWAP** > **Advanced**.

Step 2 In the **CAPWAP Window Size** field, enter the unit of measurement of the window.

Step 3 Click **Save & Apply to Device**.

Configuring AP Image Download Time Enhancement (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap-profile** *ap-profile* **Example:** `Device(config)# ap profile capwap_multiwindow`	Configures an AP profile.
Step 3	**capwap window size** *window-size* **Example:**	Configures the AP CAPWAP control packet transmit queue size.

	Command or Action	Purpose
	`Device(config-ap-profile)# capwap window size 20`	**Note** Configure the window size only for AP profiles that are exclusively used for teleworker or OEAP. Be aware that any change in window size may impact other APs.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

Verifying AP Image Download Time Enhancement Configuration

To view the CAPWAP window size present in an AP profile, use the following command:

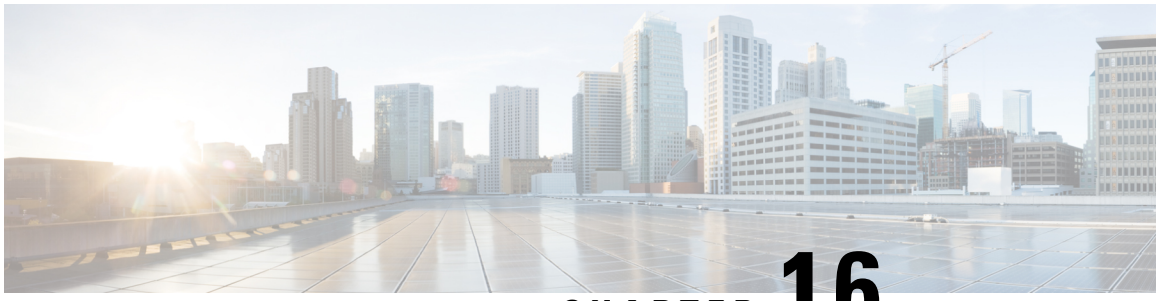
```
Device# show ap profile name default-ap-profile detailed | in wind

Capwap window size : 10
```

To view the CAPWAP status and modes, use the following command:

```
Device# show capwap client rcb

OperationState                      : UP
Name                                : AP4001.7A39.2D5A
MwarHwVer                           : 0.0.0.0
Location                            : default location
ApMode                              : Remote Bridge
ApSubMode                           : Not Configured
CAPWAP Path MTU                     : 1485
Software Initiated Reload Reason    : Reload command
CAPWAP Sliding Window
Active Window Size                  : 10
Last Request Send To Application    : 184
Expected Seq Num                    : 185
Received Seq Num                    : 184
Request Packet Count                : 42424
Out Of Range Packets Count          : 0
Window Moved  Packets Count         : 0
In Range Packets Count              : 960
Expected Packets Count              : 41464
```

To view the AP configuration details, including the CAPWAP window size, use the following command:

```
Device# show ap config general | in Wind

Capwap Active Window Size                       : 5
Capwap Active Window Size                       : 10
Capwap Active Window Size                       : 1
```



CHAPTER 16

N+1 Hitless Rolling AP Upgrade

- N+1 Hitless Rolling AP Upgrade, on page 255
- Configuring Hitless Upgrade, on page 256
- Verifying Hitless Upgrade, on page 257

N+1 Hitless Rolling AP Upgrade

The existing CAPWAP implementation on the Cisco Catalyst 9800 Series Wireless Controller requires that the controller and all its associated APs have the same software version. It is possible to upgrade a set of APs using the N+1 Hitless Rolling AP Upgrade feature. However, all the APs cannot be upgraded at the same time without network downtime.

You can upgrade wireless networks without network downtime when the same version skew is supported between the controller and the APs. This enables the APs to be upgraded in a staggered manner, while still being connected to the same controller. The version skew method can avoid upgrade downtime even for N+1 networks by using N+1 Hitless Rolling AP Upgrade feature and a spare controller.

The following is the workflow for the N+1 Hitless Rolling AP Upgrade feature:

1. Establish a mobility tunnel from the controller (WLC1) to a mobility member (WLC2).
2. Upgrade the controller software (WLC1) using the command **install add file bootflash:***new_version.bin* .
3. Optionally, you can also upgrade the AP image. For more information, see Predownloading an Image to an Access Point chapter.
4. Use the **ap image upgrade destination** *controller-name controller-ip report-name* privileged EXEC command to upgrade and move all the APs from WLC1 (source) to WLC2 (destination).
5. Activate the new image in WLC1 using the **install activate** command.
6. Commit the changes using the **install commit** command.
7. Move the APs back to WLC1 from WLC2 using the **ap image move destination** *controller-name controller-ip report-name* command.

Note The **ap image upgrade destination** command does not work without an image pre-download. If you do not perform an image pre-download, use the **ap image move** command to move the APs. When APs download the image and join the destination controller, you must set the iteration time as high. Also, you can customize the iteration time by configuring the **ap upgrade staggered iteration timeout** command.

Configuring Hitless Upgrade

Follow the procedure given below to achieve a zero downtime network upgrade in an N+1 deployment.

Before you begin

- Ensure that the hostname and wireless management IP of the destination controller is provided in the privileged EXEC command.
- Ensure that access points are predownloaded with the image running on the destination controller.

Procedure

	Command or Action	Purpose
Step 1	**ap image upgrade destination** *wlc-name wlc-ip* **Example:** `Device# ap image upgrade destination wlc2 10.7.8.9`	Moves APs to the specified destination controller with the swap and reset command. After this, the parent controller activates new image, and reloads with the new image. After the mobility tunnel comes up, APs are moved back to the parent controller without a swap and reset. **Note** Ensure that you establish a mobility tunnel from controller (WLC1) to a mobility member (WLC2) before image upgrade.
Step 2	**ap image upgrade destination** *wlc-name wlc-ip* **Example:** `Device# ap image upgrade destination wlc2 10.7.8.9`	(Optional) Moves APs to the specified destination controller with a swap and reset command. **Note** Perform Steps 2 to 4 only if you are not performing Step 1.
Step 3	**ap image move destination** *wlc-name wlc-ip* **Example:** `Device# ap image move destination wlc1 10.7.8.6`	Move the APs back to the parent controller.
Step 4	**ap image upgrade destination** *wlc-name wlc-ip* [**fallback**]	(Optional) Moves APs to the specified destination controller with a swap and reset command. After that, APs are moved back to

	Command or Action	Purpose
	Example: `Device# ap image upgrade destination wlc2 10.7.8.9 fallback`	the parent controller (without a swap and reset) after manual install activate of the new image and reloading of the parent controller.
Step 5	**ap image upgrade destination** *wlc-name wlc-ip* [**reset**] **Example:** `Device# ap image upgrade destination wlc2 10.7.8.9 reset`	(Optional) Moves APs to the specified destination controller with a swap and reset command. After this, the parent controller activates the new image and reloads with the new image.

Verifying Hitless Upgrade

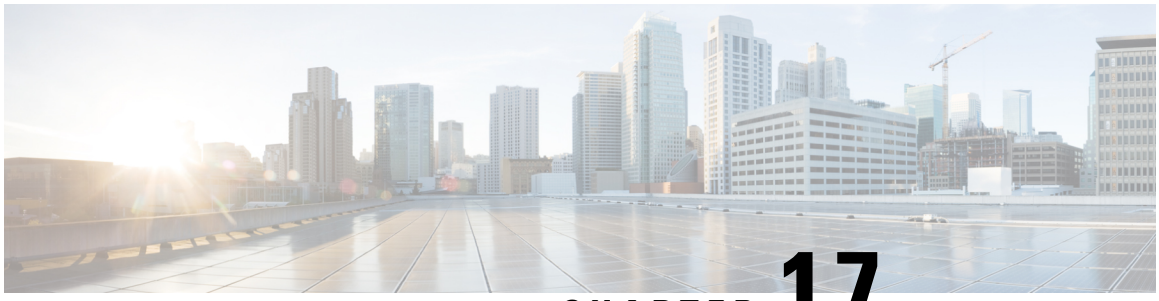
Use the following **show** commands to verify hitless upgrade.

To view all the upgrade report names, use the following command:

```
Device# show ap upgrade summary

Report Name      Start time
-----------------------------------------------------------------------------------------------
AP_upgrade_from_VIGK_CSR_2042018171639 05/20/2018 17:16:39 UTC
```

To view AP upgrade information based on the upgrade report name, use the following command:

```
Device# show ap upgrade name test-report

AP upgrade is complete
From version: 16.10.1.4
To version: 16.10.1.4
Started at: 05/20/2018 17:16:39 UTC
Percentage complete: 100
End time: 05/20/2018 17:25:39 UTC
Progress Report
---------------
Iterations
----------
Iteration Start time End time AP count
-----------------------------------------------------------------------------------------------------
0 05/20/2018 17:16:39 UTC 05/20/2018 17:16:39 UTC 0
1 05/20/2018 17:16:39 UTC 05/20/2018 17:25:39 UTC 1
Upgraded
--------
Number of APs: 1
AP Name Ethernet MAC Iteration Status
-----------------------------------------------------------------------------------------------
AP-SIDD-CLICK 70db.9848.8f60 1 Joined
In Progress
-----------
Number of APs: 0
AP Name Ethernet MAC
-------------------------------------------------
Remaining
---------
Number of APs: 0
AP Name Ethernet MAC
-------------------------------------------------
```



CHAPTER 17

Site-Based Rolling AP Upgrade in N+1 Networks

- Feature History for Site-Based Rolling AP Upgrade in N+1 Networks, on page 259
- Information About Site-Based Rolling AP Upgrade in N+1 Network, on page 259
- Prerequisites for Site-Based Rolling AP Upgrade in N+1 Networks, on page 260
- Restrictions for Site-Based Rolling AP Upgrade in N+1 Networks, on page 260
- Use Cases, on page 260
- N+1 Upgrade and Move to Destination Controller, on page 261
- N+1 Move to Destination Controller, on page 263
- Hitless Software Upgrade (N+1 Upgrade), on page 264
- Verifying Site-based Rolling AP Upgrade in a N+1 Network, on page 265

Feature History for Site-Based Rolling AP Upgrade in N+1 Networks

This table provides release and related information for the features explained in this module.

These features are available in all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 17: Feature History for Site-Based Rolling AP Upgrade in N+1 Networks

Release	Feature	Feature Information
Cisco IOS XE 17.9.1	Site-Based Rolling AP Upgrade in N+1 Network	This feature helps to achieve a zero downtime network upgrade in N+1 networks.

Information About Site-Based Rolling AP Upgrade in N+1 Network

The Site-Based Rolling AP Upgrade in an N+1 Network feature allows you to perform a staggered upgrade of APs in each site in an N+1 deployment.

This feature helps you to effectively achieve a zero-downtime network upgrade in an N+1 network. The existing site filter functionality allows you to perform a software upgrade of a site or all the sites managed by the controller.

In a typical scenario, the software of the APs belonging to a site is upgraded and the network is monitored to see whether it is functioning as intended, before adding more sites to the site filter. If the upgrade fails to meet the objectives, all the sites in the site filter can be removed using the **ap image site-filter file any-image remove-all** command. The **ap image site-filter** command is modified to include the **any-image** keyword as a substitute for the image file name to support the N+1 AP move site filter.

Prerequisites for Site-Based Rolling AP Upgrade in N+1 Networks

- The source and destination controllers should be in the same mobility group (preferably running the latest image) but with different AP image versions.
- Image of the destination controller should be available on the source controller.
- Both the source and destination controllers should be in INSTALL mode.

Restrictions for Site-Based Rolling AP Upgrade in N+1 Networks

- Site filter operations are supported only for N+1 upgrade and N+1 move; **fallback** and **reset** options of the **ap image upgrade destination** command are not supported.
- APs can only move across the controllers having the same software.
- The **any** and **remove-all** keywords of the **ap image site-filter** command work only for the N+1 AP upgrade or move. It will not work for other site filter operations such as AP Model Service Pack (APSP) or AP Device Package (APDP).
- A reboot of the source or the destination controller during the N+1 upgrade requires a re-execution of the procedure.

Use Cases

The N+1 deployments are more common compared to 1+1 redundancy deployments. In the N+1 deployments, spare controllers are used and APs can fail over to it whenever their primary controller goes down. For local mode networks, this results in a small network downtime (30 to 40 seconds), during which APs re-discover and re-join the network. However, during network upgrades, the downtime is much longer, and all the devices have to reboot and converge. The feature can effectively provide a zero-downtime network upgrade in an N+1 deployment.

N+1 Upgrade and Move to Destination Controller

Note

- Run all the commands only on the source controller.
- By default, the Rolling AP Upgrade feature sends a basic service set (BSS) transition message to 11v clients to notify them that the AP they are connected to is going down, along with a list of alternate APs. In scenarios where clients are sensitive to roaming, this feature can cause unnecessary packet drops. In such instances, you can disable the 11v message using the **no ap upgrade staggered client-steering** command.

Before you begin

See the *Prerequisites for Site-based Rolling AP Upgrade in an N+1 Network* section.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no ap upgrade staggered client-steering** **Example:** `Device# no ap upgrade staggered client-steering`	(Optional) Disables client steering.
Step 3	**ap upgrade staggered iteration completion** *min-percent* **Example:** `Device(config)# ap upgrade staggered iteration completion 50`	(Optional) Configures the minimum percentage of APs that must join the destination controller to signal iteration completion.
Step 4	**ap upgrade staggered iteration error action stop** **Example:** `Device(config)# ap upgrade staggered iteration error action stop`	(Optional) Configures the action to be taken when APs are missing after an iteration during AP upgrade.
Step 5	**ap upgrade staggered iteration timeout** *timeout-duration* **Example:** `Device(config)# ap upgrade staggered iteration timeout 18`	(Optional) Configures the maximum time allowed per iteration during AP upgrade. Valid values range from 9 to 60.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 7	**ap image site-filter any-image add** *site-tag* **Example:** `Device# ap image site-filter any-image add site1`	Adds a site tag to a site filter. You can repeat this step to set up a multisite filter.
Step 8	**ap image move destination** *controller-name controller-ip* **Example:** `Device# ap image move destination controller2 10.9.34.4`	Moves the APs to a different controller in the mobility group. **Note** It is preferable to move the APs to a different controller running the same image. Wait for the upgrade to complete. If upgrade is not completed successfully, you can use the **ap image upgrade destination** or **ap image move destination** commands to restart the upgrade process.
Step 9	**ap image site-filter any-image add** *site-tag* **Example:** `Device# ap image site-filter file any-image add site2`	Adds additional site tag to a site filter.
Step 10	**ap image site-filter any-image apply** **Example:** `Device# ap image site-filter file any-image apply`	Predownloads the image and upgrades the APs based on the site filter. **Note** Wait for the upgrade to complete.
Step 11	**ap image site-filter any-image clear** **Example:** `Device# ap image site-filter file any-image clear`	(Optional) Clears the site filter table and predownloads the image and does a rolling AP upgrade to all the sites.
Step 12	**ap image site-filter file any-image remove-all** **Example:** `Device# ap image site-filter file any-image remove-all`	(Optional) Removes all the site filters.

N+1 Move to Destination Controller

Note Run all the commands only on the source controller.

Before you begin

See the *Prerequisites for Site-based Rolling AP Upgrade in an N+1 Network* section.

Procedure

	Command or Action	Purpose
Step 1	**ap image site-filter any-image add** *site-tag* **Example:** `Device# ap image site-filter any-image add site1`	Adds a site tag to a site filter.
Step 2	**ap image move destination** *image-name controller-ip* **Example:** `Device# ap image move destination controller2 10.9.34.2`	Moves the APs back to the parent controller. **Note** Wait for the upgrade to complete.
Step 3	**ap image site-filter any-image add** *site-tag* **Example:** `Device# ap image site-filter any-image add site2`	Adds an additional site tag to a site filter.
Step 4	**ap image site-filter any-image apply** **Example:** `Device# ap image site-filter any-image apply`	Upgrades the APs based on the site filter. **Note** Wait for the upgrade to complete. If upgrade is not completed successfully, use the **ap image upgrade destination** or **ap image move destination** command to restart the upgrade process.
Step 5	**ap image site-filter any-image clear** **Example:** `Device# ap image site-filter any-image clear`	(Optional) Clears the site filter table and predownloads the image and does a rolling AP upgrade to all the sites where it is not active.

Hitless Software Upgrade (N+1 Upgrade)

Hitless software upgrade uses the concept of N+1 high availability using a spare controller to upgrade the CAPWAP infrastructure comprising controllers and access points (AP). Depending on what you choose, the APs are upgraded in a staggered fashion, per site, or on all sites , using the Rolling AP upgrade feature thereby avoiding network disruption. This ensures that the clients are serviced by the neighboring APs while one or the selected APs undergo the upgrade process.

The upgrade workflow is as follows :

1. Initiate upgrade on the source controller. You can choose to upgrade all sites or per site based on your preference.
2. Move the APs to the destination controller. APs are upgraded in a staggered fashion using the rolling AP upgrade algorithm.
3. Once all the APs move to the destination controller in multiple iterations, activate the target image on the source controller.
4. The source controller reloads for the new image to take effect.
5. (Optional) Move the APs back to the source controller using the cli commands.

Before you begin

- The controller should be in INSTALL mode.
- The controller should be paired with another controller and both should be part of the same mobility group.

  The spare controller should be upgraded with the target image.

Procedure

Step 1 Choose **Administration > Software Management** .

Step 2 From the Software Upgrade tab check the **One-Shot Install Upgrade** checkbox.

Step 3 From the **Transport Type** drop-down list, choose an option.

a) If you choose **My Desktop** as the transport type, click **Select File** to navigate to the file from the **Source File Path** field.

b) If you choose **SFTP** as the transport type, enter the source IP address, SFTP username, SFTP password, file path, and select the destination.

c) If you choose **FTP** as the transport type, enter the source IP address, FTP username, FTP password, file path, and select the destination.

d) If you choose **TFTP** as the transport type, enter the source IP address, file path, and select the destination.

Note In controllers, the IP TFTP source is mapped to the service port by default.

e) If you choose **Device** as the transport type, choose the file system and file path.

Note In the **File Path** field, enter the complete path from where you want to download the software image file, including the name of the file.

Step 4 Check the **Enable Hitless Upgrade** check box to allow the APs and the controller to be upgraded.

Step 5 From the **Site Filter** drop-down list, choose **All Sites** or one or more **Custom Sites**.

In case you choose to upgrade for **All Sites**, you can optionally enable **Fallback after Upgrade** so that the APs move back to the parent controller after the new image has been activated and the parent controller has reloaded.

In case you choose a **Custom Site**, select the site from the **Site Tags** drop-down list. In this case, the APs do not move back to the parent controller automatically and you will have to manually move them using CLIs.

Step 6 In the **Controller IP Address (IPv4/IPv6)** field, enter the source controller's IPv4/IPv6 address.

Step 7 In the **Controller Name** field, enter the source controller's name.

Step 8 In the **AP Upgrade Configuration** section, use the **AP Upgrade per Iteration** drop-down list to select the percentage of APs to be upgraded per iteration. This configures the minimum percentage of APs that must join the destination controller to signal completion of iteration.

Step 9 Check the **Client Steering** check box to move clients attached to APs undergoing an upgrade to other APs. If the clients still persist on the candidate APs, they are disconnected and the APs will reload with the new image.

Step 10 In the **Accounting Percentage** field, choose the percentage of APs that should join the destination controller after each iteration (of the staggered AP upgrade) to consider the iteration as successful. The default value is 90%.

Step 11 Tap to select the type of **Accounting Action** to configure for the APs. If you enable **Terminate**, the upgrade is terminated if the configured percentage of APs does not join the mobility peer, and a notification is sent via Syslog message. If you choose **Ignore**, the upgrade continues irrespective of whether the configured percentage of APs are joining the controller or not.

Step 12 In the **Iteration Expiry** field, select the number of minutes from the drop-down list to configure the expiry time for each iteration.

Step 13 Click **Download & Install**.

Step 14 Click **Save Configuration & Activate**.

Step 15 Click **Commit** to make the activation changes persistent across reloads.

Verifying Site-based Rolling AP Upgrade in a N+1 Network

Use the following **show** commands to check the progress of the upgrade and debugging:

- **show ap summary**
- **show ap tag summary**
- **show ap status**
- **show wireless mobility summary**
- **show ap image**
- **show ap upgrade**
- **show ap upgrade site**
- **show ap upgrade site summary**

- **show ap upgrade name** *report-name*
- **show wireless mobility ap-list**

To view the summary of all the connected Cisco APs, use the following command:

```
Device# show ap summary

Number of APs: 8

AP Name             Slots  AP Model           Ethernet MAC    Radio MAC       Location
       Country  IP Address    State
-------------------------------------------------------------------------------------------
AP00D7.8F9A.43DE    2      AIR-AP2802I-D-K9   00d7.8f9a.43de  002c.c8df.3ca0  default
location    IN       10.9.48.254  Registered
AP4C77.6D21.9098    2      AIR-AP2802E-N-K9   4c77.6d21.9098  00be.7573.b340  default
location    IN       10.10.10.52  Registered
AP00F2.8B27.BB2C    2      AIR-AP2802I-D-K9   00f2.8b27.bb2c  0896.ad9b.f9e0  default
location    IN       10.9.44.51   Registered
APA023.9F41.5A38    2      AIR-AP2802I-D-K9   a023.9f41.5a38  1880.90f4.7b00  default
location    IN       10.10.10.51  Registered
AP00A3.8E4A.762C    2      AIR-AP2802I-D-K9   00a3.8e4a.762c  1880.90f5.14e0  default
location    IN       10.9.48.54   Registered
AP40CE.2485.D616    2      AIR-AP3802I-D-K9   40ce.2485.d616  4001.7aca.5960  default
location    IN       10.9.50.42   Registered
AP40CE.2485.D62C    2      AIR-AP3802I-D-K9   40ce.2485.d62c  4001.7aca.5aa0  default
location    IN       10.10.10.53  Registered
AP2C57.4188.4BC4    3      C9130AXE-D         2c57.4188.4bc4  cc7f.75a8.78e0  default
location    IN       10.9.34.207  Registered
```

To view the summary of all the access points with policy tags, use the following command:

```
Device# show ap tag summary
Number of APs: 8

AP Name             AP Mac           Site Tag Name     Policy Tag Name       RF Tag Name
     Misconfigured    Tag Source
-------------------------------------------------------------------------------------------
AP00D7.8F9A.43DE    00d7.8f9a.43de   site3             default-policy-tag   default-rf-tag
    No               Static
AP4C77.6D21.9098    4c77.6d21.9098   site3             default-policy-tag   default-rf-tag
    No               Static
AP00F2.8B27.BB2C    00f2.8b27.bb2c   site3             default-policy-tag   default-rf-tag
    No               Static
APA023.9F41.5A38    a023.9f41.5a38   default-site-tag   default-policy-tag   default-rf-tag
    No               Default
AP00A3.8E4A.762C    00a3.8e4a.762c   site1             default-policy-tag   default-rf-tag
    No               Static
AP40CE.2485.D616    40ce.2485.d616   site2             default-policy-tag   default-rf-tag
    No               Static
AP40CE.2485.D62C    40ce.2485.d62c   site2             default-policy-tag   default-rf-tag
    No               Static
AP2C57.4188.4BC4    2c57.4188.4bc4   default-site-tag   default-policy-tag   default-rf-tag
    No               Default
```

To view the status of the access points, use the following command:

```
Device# show ap status
AP Name                              Status     Mode              Country
-------------------------------------------------------------------------------
```

```
AP00A3.8E4A.762C                    Enabled    Local            IN
AP00D7.8F9A.43DE                    Enabled    Monitor          IN
AP00F2.8B27.BB2C                    Enabled    Local            IN
AP2C57.4188.4BC4                    Enabled    Local            IN
AP40CE.2485.D616                    Enabled    Local            IN
AP40CE.2485.D62C                    Enabled    Local            IN
AP4C77.6D21.9098                    Enabled    Local            IN
APA023.9F41.5A38                    Enabled    Local            IN
```

To display the summary of the mobility manager, use the following command:

```
Device# show wireless mobility summary

Mobility Summary

Wireless Management VLAN: 34
Wireless Management IP Address: 10.9.34.5
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384,
 TLS_RSA_AES128_CBC_SHA
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: mobility-1
Mobility Multicast Ipv4 address: 10.0.0.1
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.14a5.b3ff
Mobility Domain Identifier: 0x39ab

Controllers configured in the Mobility Domain:

 IP        Public Ip  MAC Address    Group Name  Multicast IPv4 Multicast IPv6  Status
PMTU
-------------------------------------------------------------------------------------------
10.9.34.5  N/A        001e.14a5.b3ff mobility-1  0.0.0.0        ::              N/A     N/A
10.9.34.2  10.9.34.2   001e.bd2d.f2ff mobility-1  0.0.0.0        ::              Up
1385
10.9.34.3  10.9.34.3   001e.14c1.cbff mobility-1  0.0.0.0        ::              Up
1385
10.9.34.4  10.9.34.4   001e.140e.4bff mobility-1  0.0.0.0        ::              Up
1385
```

To view the cumulative statistics regarding the AP images in the controller, use the following command:

```
Device# show ap image

Total number of APs  : 8


Number of APs
        Initiated                : 0
        Downloading              : 0
        Predownloading           : 0
        Completed downloading    : 0
        Completed predownloading : 0
        Not Supported            : 0
        Failed to Predownload    : 0
        Predownload in progress  : No
AP Name           Primary Image Backup Image Predownload Status Predownload Version  Next
Retry Time Retry Count  Method
-------------------------------------------------------------------------------------------------
AP00D7.8F9A.43DE  17.9.0.19     17.8.0.74    None               0.0.0.0             N/A
            0           N/A
```

```
AP4C77.6D21.9098  17.9.0.19     17.8.0.74    None                0.0.0.0             N/A
            0           N/A
AP00F2.8B27.BB2C  17.9.0.19     17.9.1.19    None                0.0.0.0             N/A
            0           N/A
APA023.9F41.5A38  17.9.0.19     17.8.0.74    None                0.0.0.0             N/A
            0           N/A
AP00A3.8E4A.762C  17.9.0.19     17.9.1.19    None                0.0.0.0             N/A
            0           N/A
AP40CE.2485.D616  17.9.0.19     17.9.1.19    None                0.0.0.0             N/A
            0           N/A
AP40CE.2485.D62C  17.9.0.19     17.8.0.82    None                0.0.0.0             N/A
            0           N/A
AP2C57.4188.4BC4  17.9.0.19     17.9.1.19    None                0.0.0.0             N/A
            0           N/A
```

To verify the AP upgrade on the controller, use the following command:

```
Device# show ap upgrade

AP upgrade is in progress

From version: 17.9.0.19
To version: 17.9.1.25

Started at: 01/28/2022 09:53:07 IST
Configured percentage: 5
Percentage complete: 0
Expected time of completion: 01/28/2022 13:33:07 IST

Client steering: Enabled
Iteration expiry time: 15 minutes
Accounting percentage: 95%
Accounting action: Abort

Rolling AP Upgrade Site Summary
-------------------------------
site3

Progress Report
---------------
Iterations
----------
Iteration       Start time                  End time                    AP count
-------------------------------------------------------------------------------------
0               01/28/2022 09:53:07 IST     01/28/2022 09:53:07 IST     1
1               01/28/2022 09:53:07 IST     ONGOING                     0

Upgraded
--------
Number of APs: 1
AP Name                 Radio MAC       Iteration   Status     Site
-------------------------------------------------------------------------------------
AP00D7.8F9A.43DE        002c.c8df.3ca0  0           Rebooted    site3

In Progress
-----------
Number of APs: 1
AP Name                          Radio MAC
-------------------------------------------------
AP00F2.8B27.BB2C                 0896.ad9b.f9e0

Remaining
---------
Number of APs: 1
```

```
AP Name                          Radio MAC
-----------------------------------------------
AP4C77.6D21.9098                 00be.7573.b340

APs not handled by Rolling AP Upgrade
-------------------------------------
AP Name      Radio MAC           Status          Reason for not handling by Rolling AP
Upgrade
-----------------------------------------------------------------------------------------------------
```

To verify the AP upgrade information on the sites, use the following command:

```
Device# show ap upgrade site

Site-filtered AP upgrade report data
====================================
Source controller: Controller1
Destination controller: Controller2

From version: 17.9.0.19
To version: 17.9.1.25
Site-filters present: Yes

AP image upgrade site summary
-----------------------------
Operation: N+1 upgrade

Site Tag                                    Status
------------------------------------------------------------
site3                                       In Progress

AP upgrade reports linked to these site-filters
-----------------------------------------------

Start time               Operation type             Report name
-------------------------------------------------------------------------------
01/28/2022 09:53:07 IST  AP image upgrade/move CLI  AP_upgrade_to_DEvice2_28020229536
```

To verify the AP image upgrade site summary, use the following command:

```
Device# show ap upgrade site summary

AP image upgrade site summary
-----------------------------
Operation: N+1 upgrade

Site Tag                                    Status
------------------------------------------------------------
site3                                       In Progress
```

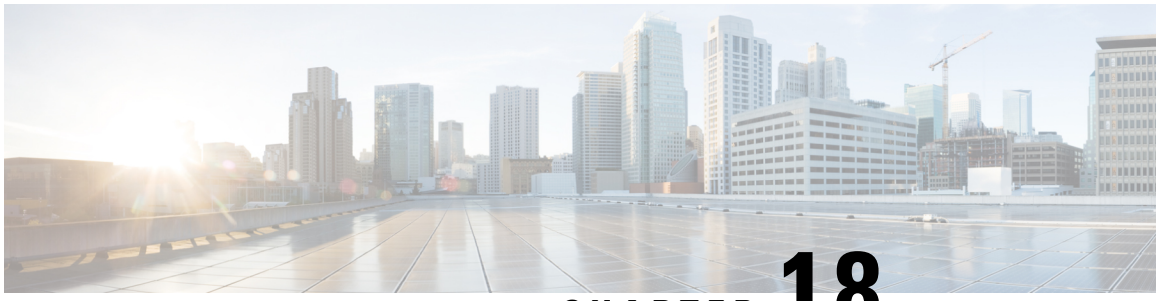
To view AP upgrade information based on the upgrade report name, use the following command:

```
Device# show ap upgrade name AP_upgrade_to_Device2

AP upgrade is complete

From version: 17.9.0.19
To version: 17.9.1.25

Started at: 01/28/2022 14:12:49 IST
Configured percentage: 5
Percentage complete: 100
End time: 01/28/2022 14:18:59 IST
```

```
Client steering: Enabled
Accounting percentage: 95%
Iteration expiry time: 15 minutes
Accounting action: Abort

Rolling AP Upgrade Site Summary
-------------------------------
site1
site2

Progress Report
---------------
Iterations
----------
Iteration     Start time                    End time                    AP count
-------------------------------------------------------------------------------------
0             01/28/2022 14:12:49 IST       01/28/2022 14:12:49 IST     0
1             01/28/2022 14:12:49 IST       01/28/2022 14:15:54 IST     1
2             01/28/2022 14:15:54 IST       01/28/2022 14:18:59 IST     1

Upgraded
--------
Number of APs: 2
AP Name               Radio MAC         Iteration  Status          Site
-------------------------------------------------------------------------------------------
AP40CE.2485.D616      4001.7aca.5960    1          Joined Member   site2
AP40CE.2485.D62C      4001.7aca.5aa0    2          Joined Member   site2

In Progress
-----------
Number of APs: 0
AP Name                           Radio MAC
-------------------------------------------------

Remaining
---------
Number of APs: 0
AP Name                           Radio MAC
-------------------------------------------------

APs not handled by Rolling AP Upgrade
-------------------------------------
AP Name      Radio MAC      Status    Reason for not handling by Rolling AP Upgrade
-------------------------------------------------------------------------------------------
```

To display the list of access points known to the mobility group, use the following command:

```
Device# show wireless mobility ap-list

AP name                            AP radio MAC      Controller IP     Learnt from
-------------------------------------------------------------------------------------
Unknown                            002c.c8df.3ca0    10.9.34.5          Self
Unknown                            00be.7573.b340    10.9.34.5          Self
Unknown                            0896.ad9b.f9e0    10.9.34.5          Self
Unknown                            1880.90f4.7b00    10.9.34.5          Self
Unknown                            1880.90f5.14e0    10.9.34.5          Self
Unknown                            4001.7aca.5960    10.9.34.5          Self
Unknown                            4001.7aca.5aa0    10.9.34.5          Self
Unknown                            687d.b45e.4b60    10.9.34.3          Mobility Group
Unknown                            cc7f.75a8.78e0    10.9.34.5          Self
```



CHAPTER 18

NBAR Dynamic Protocol Pack Upgrade

- NBAR Dynamic Protocol Pack Upgrade, on page 271
- Upgrading the NBAR2 Protocol Pack, on page 272

NBAR Dynamic Protocol Pack Upgrade

Protocol packs are software packages that update the Network-Based Application Recognition (NBAR) engine protocol support on a device without replacing the Cisco software on the device. A protocol pack contains information on applications that are officially supported by NBAR, and are compiled and packed together. In each application, the protocol pack includes information on application signatures and application attributes. Each software release has a built-in protocol pack bundled with it.

The Application Visibility and Control (AVC) feature (used for deep-packet inspection [DPI]) supports wireless products using a distributed approach that benefits from NBAR running on the access points (AP) or controller whose goal is to run DPI and report the result using NetFlow messages.

The AVC DPI technology supports the ability to update recognized traffic and to define the custom type of traffic (known as custom applications). The NBAR runs on the controller in local mode, and on the APs in Flex and Fabric modes. In local mode, all the traffic coming from the APs are tunneled towards the wireless controller.

Note

- Although NBAR is supported in all the modes, upgrade of NBAR protocol packs is supported only in local mode (central switching) and in FlexConnect mode (central switching).
- Custom applications are available only in local mode (central switching) and in FlexConnect mode (central switching).
- When you upgrade the AVC protocol pack, copy the protocol pack to both RPs (active and standby). Otherwise, the protocol pack on the standby upgrade will fail and cause the synchronization failure crash.

Protocol packs provide the following features:

- They can be loaded easily and quickly.
- They can be upgraded to a later version protocol pack or revert to an earlier version protocol pack.
- Device reload is not required.

- They do not disrupt any service.

Protocol Pack Upgrade

Using protocol pack upgrades, you can update the NBAR engine to recognize new types of protocols or traffic without updating the entire switch or appliance image. It also eliminates the need to restart the entire system.

NBAR protocol packs are available for download from Cisco Software Center: https://software.cisco.com/download/navigator.html

Custom Applications

Using custom applications, you can force the NBAR engine to recognize traffic based on a set of custom rules, for example, destination IP, hostname, URL, and so on.

The custom application names then appear in the web UI or in the NetFlow collector.

Upgrading the NBAR2 Protocol Pack

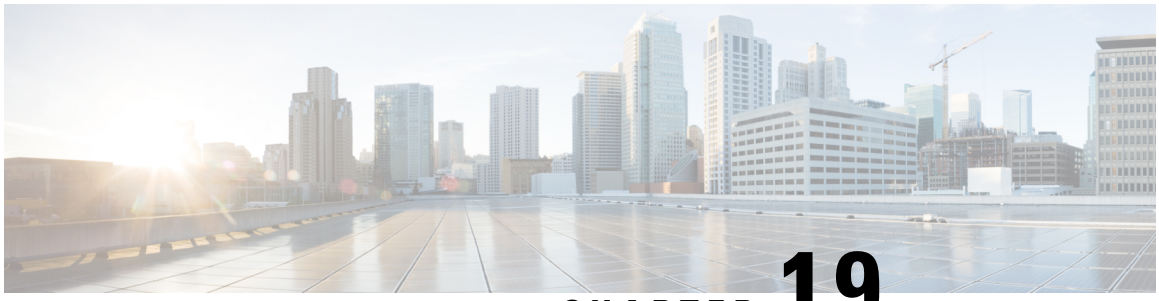
Follow the procedure given below to upgrade the NBAR2 protocol pack:

Before you begin

Download the protocol pack from Software Download page and copy it into the bootflash.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip nbar protocol-pack bootflash:***pack-name* **Example:** `Device(config)# ip nbar protocol-pack bootflash:mypp.pack`	Loads the protocol pack.



CHAPTER 19

Wireless Sub-Package for Switch

- Introduction to Wireless Sub-package, on page 273
- Booting in Install Mode, on page 274
- Installing Sub-Package in a Single Step (GUI), on page 275
- Installing Sub-Package in a Single Step, on page 275
- Multi-step Installation of Sub-Package, on page 276
- Installing on a Stack, on page 276
- Upgrading to a Newer Version of Wireless Package, on page 277
- Deactivating the Wireless Package, on page 277
- Enabling or Disabling Auto-Upgrade, on page 277

Introduction to Wireless Sub-package

Wireless-only Fabric uses fabric constructs to garner the benefits of a fabric. In this architecture, a fabric is built on top of existing traditional network designs such as multi-tier, Routed Access, and VSS network. It uses a LISP control plane together with VXLAN encapsulation for the overlay data plane traffic. The wireless control plane remains intact with CAPWAP tunnels initiating on the APs and terminating on a Cisco Catalyst 9800 Series Wireless Controller or AireOS controller. The Cisco Catalyst 9800 Series Wireless Controller can function in a dedicated appliance, directly in a switch, or in a VM.

Cisco Catalyst 9800 Wireless Controller for Switch delivers all the benefits of a centralized control and management plane (easy to configure, upgrade, troubleshoot, etc) and the maximum throughput or performance of a distributed forwarding plane. The distributed data plane allows services such as AVC to scale. In this new model, the wireless control plane is not split between MC and MA. The switch is detached from the wireless control plane and the controller takes care of the wireless function and the traffic switching is done by the Cisco Access Switch.

Since the wireless functionality is required to be enabled only on few nodes of the network, you can install Cisco Catalyst 9800 Series Wireless Controller as a separate package on the switch on a need basis. The sub-package is installed on top of the base image and a reload is required to activate the sub-package.

Note The sub-package is an optional binary that contains the entire Cisco Catalyst 9800 Series Wireless Controller software.

Note SNMP is not supported on Catalyst 9800 Embedded Wireless Controller for Switch.

How to Install Wireless Package

1. Install the base image (without wireless) on the switch.
2. Install the wireless package on the switch.
3. Upgrade the AP image.
4. Reload the switch.
5. Enable wireless on the switch using the **wireless-controller** configuration command, and configure wireless features.

How to Remove Wireless Package

1. Uninstall the wireless package from the switch.
2. Reload the switch.
3. Run the **write** command. This removes the wireless configuration from the startup-configuration.

Upgrading to a Newer Version of Wireless Package

1. Install the base image (without wireless) on the switch.
2. Install the updated wireless package.
3. Reload the switch.
4. Commit the installation.

Booting in Install Mode

Use the procedure given below to boot the switch in install-mode:

Before you begin

The sub-package does not work in bundle-mode. Use the **show version** command to verify the boot mode.

Procedure

Step 1 **install add file** *image.bin location* **activate commit**.

This command moves the switch from bundle-mode to install-mode. Note that *image.bin* is the base image.

Step 2 Click **yes** to all the prompts.

Step 3 **reload**

Reloads the switch. Ensure that you boot from *flash:packages.conf*. After the reload, the switch will be in install-mode.

Note During Install mode image upgrade/downgrade, “Install add file” with flash:<file_name> command is not supported. Instead of that “bootflash:<filename”> needs to be used.

```
Install add file bootflash:<file_name>  activate commit
```

What to do next

Verify the boot mode using the **show version** command.

Installing Sub-Package in a Single Step (GUI)

Procedure

Step 1 Choose **Administration** > **Software Management** > **Software Upgrade**.

Step 2 Choose the upgrade mode from the **Upgrade Mode** drop-down list, the transport type from the **Transport Type** drop-down list and enter the **Server IP Address (IPv4/IPv6)**, the **File System** and choose the location from the **Source File Path** drop-down list.

Step 3 Click **Download & Install**.

Installing Sub-Package in a Single Step

Use the procedure given below to install sub-package in a single step:

Before you begin

- Ensure that the switch is in install-mode.
- Ensure that you boot only from *flash:packages.conf*.

Procedure

Step 1 **install add file** *flash:<controller>.bin* **activate commit**

Installs the Cisco Catalyst 9800 Wireless Controller for Switch sub-package.

Note The sub-package (flash:<controller>.bin) is available on www.cisco.com. You can also install the sub-package directly from TFTP server.

Step 2 Click **yes** to all the prompts.

What to do next

Use the **show install summary** command to verify the installed image or package.

Multi-step Installation of Sub-Package

Use the procedure given below to install sub-package:

Before you begin

- Ensure that the switch is in install-mode.
- Ensure that you boot only from *flash:packages.conf*.

Procedure

Step 1 **install add file** *flash:<controller>.bin*

The sub-package is added to the flash and expanded.

Step 2 **install activate file** *flash:<controller>.bin*

Installs the sub-package.

Step 3 **install commit**

Completes the installation by writing the files.

What to do next

Use the **show install summary** command to verify the installed image or package.

Installing on a Stack

You can install the package on a stack using either Single-step Package Installation or #unique_336.

If a new member joins the stack, the two possible scenarios are:

- **If auto-upgrade is enabled**: The required software is installed on to the new member. It will match the version of software running on the stack as well as the wireless package.
- **If auto-upgrade is disabled**: As the software version is not the same as in the stack, the new member will remain in version mismatch state and it will not join the stack. You have to manually run the **install autoupgrade** command in EXEC mode to initiate the auto-upgrade procedure.

Upgrading to a Newer Version of Wireless Package

Use the procedure given below to upgrade to a newer version of wireless package:

Procedure

Step 1 **install add file** *flash:<base-image>.bin*

The base image (without wireless) is added to the flash and expanded.

Step 2 **install add file** *flash:<controller-sub-package>.bin*

The sub-package is added to the flash and expanded.

Step 3 **install active**

Installs the base image and sub-package and triggers a reload. However, you can also rollback to the previous state after the reload.

Step 4 **install commit**

Completes the installation by writing the files.

Deactivating the Wireless Package

Follow the procedure given below to deactivate the wireless sub-package:

Procedure

	Command or Action	Purpose
Step 1	**install deactivate file** *flash:<controller>.bin* **Example:** `Device# install deactivate file flash:<controller>.bin`	Removes the package and forces the switch to reboot.
Step 2	**install commit** **Example:** `Device# install commit`	Commits the switch without wireless package.

Enabling or Disabling Auto-Upgrade

Follow the procedure given below to enable or disable auto-upgrade:

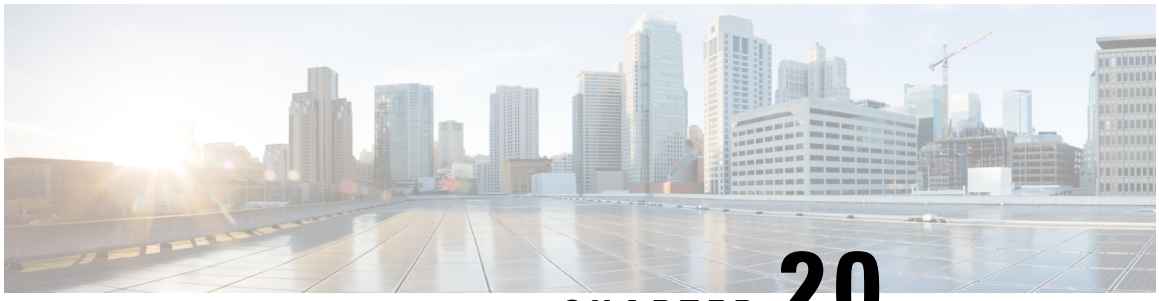
Procedure

	Command or Action	Purpose
Step 1	**software auto-upgrade enable** **Example:** `Device(config)# software auto-upgrade enable`	Enables software auto-upgrade.
Step 2	**no software auto-upgrade enable** **Example:** `Device(config)# no software auto-upgrade enable`	Disables software auto-upgrade.

PART III

Lightweight Access Points

- Countries and Regulations, on page 281
- Access Points Modes , on page 307
- Security, on page 387
- AP Joining, on page 399
- AP Management, on page 407
- AP Configuration, on page 445
- Troubleshooting Lightweight Access Points, on page 487



CHAPTER 20

Countries and Regulations

- Information About Country Codes, on page 281
- Prerequisites for Configuring Country Codes, on page 281
- Configuring Country Codes (GUI), on page 282
- Configuring Country Codes (CLI), on page 282
- Configuration Examples for Configuring Country Codes, on page 284
- Information About Regulatory Compliance Domain, on page 285
- Configuring Country Code for Rest of the World (CLI) , on page 305

Information About Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Information About Japanese Country Codes

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- J2: Allows only -P radios to join the controller
- J4: Allows 2.4G JPQU and 5G PQU to join the controller.

Prerequisites for Configuring Country Codes

- Generally, you should configure one country code per device; you configure one code that matches the physical location of the device and its access points. You can configure up to 200 country codes per device. This multiple-country support enables you to manage access points in various countries from a single device.
- When the multiple-country feature is used, all the devices that are going to join the same RF group must be configured with the same set of countries, configured in the same order.

- Access points are capable of using all the available legal frequencies. However, access points are assigned to the frequencies that are supported in their relevant domains.
- The country list configured on the RF group leader determines which channels the members will operate on. This list is independent of which countries have been configured on the RF group members.
- For devices in the Japan regulatory domain, you should have one or more Japan country codes (JP, J2, or J3) configured on your device at the time you last booted your device.
- For devices in the Japan regulatory domain, you should have one or more Japan country codes (J2, or J4) configured on your device at the time you last booted your device.
- For devices in the Japan regulatory domain, you must have at least one access point with a -J regulatory domain joined to your device.
- You cannot delete any country code using the configuration command **wireless country country-code** if the specified country was configured using the **ap country list** command and vice-versa.

Configuring Country Codes (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **Country**.

Step 2 On the **Country** page, select the check box for each country where your access points are installed. If you selected more than one check box, a message is displayed indicating that RRM channels and power levels are limited to common channels and power levels.

Step 3 Click **Apply**.

Configuring Country Codes (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**show wireless country supported** **Example:** `Device# show wireless country supported`	Displays a list of all the available country codes.
Step 3	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 4	**ap dot11** { **24ghz** | **5ghz** | **6ghz** } **shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the 802.11b/g network, if you use 24ghz. Disables the 802.11a network, if you use 5ghz. Disables the 802.11 6GHz network, if you use 6ghz.
Step 5	**ap country** *country_code* **Example:** `Device(config)# ap country IN`	Configures country code on the controller, so that access points joining controller matches the country code and its corresponding regulatory domain codes for the AP. **Note** More than one country code can be configured.
Step 6	**wireless country** *country_code* **Example:** `Device(config)# wireless country IN`	Configures 200 country codes per device. **Note** This CLI is applicable for deployments having more than 20 countries.
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 8	**show wireless country configured** **Example:** `Device# show wireless country configured`	Displays the configured countries.
Step 9	**show wireless country channels** **Example:** `Device# show wireless country channels`	Displays the list of available channels for the country codes configured on your device. **Note** Perform Steps 9 through 17 only if you have configured multiple country codes in Step 6.
Step 10	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 11	**no ap dot11** { **24ghz** | **5ghz** | **6ghz** } **shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Enables the 802.11b/g network, if you use 24ghz. Enables the 802.11a network, if you use 5ghz. Enables the 802.11 6-GHz network, if you use 6ghz.

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 13	**ap name** *cisco-ap* **shutdown** **Example:** `Device# ap name AP02 shutdown`	Disables the access point. **Note** Ensure that you disable only the access point for which you are configuring country codes.
Step 14	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 15	**ap name** *cisco-ap* **country** *country_code* **Example:** `Device# ap name AP02 country US`	Assigns each access point with a country code from the controller country code list. **Note** • Ensure that the country code that you choose is compatible with the regulatory domain of at least one of the access point's radios. • Disable the access point before changing country code.
Step 16	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 17	**ap name** *cisco-ap* **no shutdown** **Example:** `Device# ap name AP02 no shutdown`	Enables the access point.

Configuration Examples for Configuring Country Codes

Viewing Channel List for Country Codes

This example shows how to display the list of available channels for the country codes on your device:

```
Device# show wireless country channels

Configured Country.....................: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
```

```
     A = Channel is the Auto-RF default in this country.
     . = Channel is not legal in this country.
     C = Channel has been configured for use by Auto-RF.
     x = Channel is available to be configured for use by Auto-RF.
  (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11bg         :
Channels         :                  1 1 1 1 1
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US    : A * * * * A * * * * A . . .
Auto-RF          : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11a          :                        1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels         :3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                  4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US    : . A . A . A . A A A A A * * * * * . . . * * * A A A A*
Auto-RF          : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
4.9GHz 802.11a   :
Channels         :                  1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
US (-A ,-AB )    : * * * * * * * * * * * * * * * * * * * A * * * * * A
Auto-RF          : . . . . . . . . . . . . . . . . . . . . . . . . . .
```

Information About Regulatory Compliance Domain

Controllers and access points (AP) are designed for use in many countries with varying regulatory requirements. Country code enables to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

This feature helps to reduce the number of regulatory domains by modifying the existing pre-provision domains workflow to determine the regulatory domain at runtime for each country code. A new Rest of World (RoW) domain has been introduced and merged to include the nine pre-existing domains. Every AP can determine its own regulatory domain from one of these domains, with the regulated power table and the allowed radio channels.

Note The transmission power value in the TPC IE of the beacon can differ from that of the transmission power value of the AP displayed in the **show controllers dot11radio** command, by a maximum difference of 2 dB. The maximum deviation allowed in TPC IE of beacon is 2 dB.

Global Country-Level Domains

Table 18: Power Table and Supported Channels of Countries in Global Domain (2.4-GHz and 5-GHz)

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4-GHz	Supported Primary Channels 5-GHz	Supported Secondary Channels 5-GHz
Albania: AL	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	NA	100-104-108-112-116-132-136-140
Australia: Au	2G-A	5G-Z	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60-64-100-104-108-112-116-132-136-140-149-153-157-161-165	100-104-108-112-116-132-136-140-149-153-161-165
Austria: AT	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108 112-116-132-136-140
Belgium: BE	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Bulgaria: BG	2G-E	5G-E	1-2-3-4-5-6, 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Canada: CA	2G-A	5G-A	1-2-3-4-5-6 7-8-9-10-11	36-40-44-48-52-56-60-64-100-104-108-112-116-132-136-140-149-153-157-161-165	100-104-108-112-116-132-136-140-149-153-157-161-165
China: CN			1-2-3-4-5-6, 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-149-153-157-161-165	149-153-157-161-165
Croatia: HR	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Cyprus: CY	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Czech Republic: CZ	2G-E	5G-E	1-2-3-4-5-6-7-8-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Denmark: DK	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Estonia: EE	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4-GHz	Supported Primary Channels 5-GHz	Supported Secondary Channels 5-GHz
Finland: FI	2G-E	5G-E	1-2,-3-4-5 6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108 112-116-132-136-140
France: FR	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108- 112-116-132-136-140
Germany: DE	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108- 112-116-132-136-140
Gibraltar	NA	NA	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108- 112-116-132-136-140
Greece: GR	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108- 112-116-132-136-140
Hungary: HU	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108 112-116-132-136-140
Iceland: IS	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108 112-116-132-136-140
Indonesia: ID	2G-F	5G-F	1-2-3-4-5-6 7-8-9-10-11-12-13	NA	149-153-157-161
Israel: IL[7]	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	NA	1-2-3-4-5-6-7-8-9-10-11-12-13-36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140
Italy: IT	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108 112-116-132-136-140
Japan: JP	2G-Q	5G-Q	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140-144	100-104-108- 112-116-120-124-128-132-136-140-144
Korea: KR	NA	NA	1-2-3-4-5-6 7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165	100-104-108 112-116-132-136-140-149-153-157-161-165
Latvia: LV	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108 112-116-132-136-140
Liechtenstein: LI	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108- 112-116-132-136-140

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4-GHz	Supported Primary Channels 5-GHz	Supported Secondary Channels 5-GHz
Lithuania: LT	2G-E	5G-E	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Luxembourg: LU	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108 112-116-132-136-140
Malta: MT	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Mexico: MX	NA	NA	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165	100-104-108 112-116-132-136-140-149-153-157-161-165
Monaco: MN	NA	NA	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Netherlands: NL	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
New Zealand: NZ	2G-A	5G-E	1-2-3-4-5-6-7-8-9-10-11	NA	100-104-108-112-116-132-136-140-149-153-161-165
Norway: NO	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Poland: PL	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Portugal: PT	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Puerto Rico: PR	2G-A	5G-B	1-2-3-4-5-6-7-8-9-10-11	NA	36-40-44-48-52-56-60-64-100-104-108-112-116-120-128-132-140-144-149-153-157-161-165
Romania: RO	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4-GHz	Supported Primary Channels 5-GHz	Supported Secondary Channels 5-GHz
Russian Federation: RU	2G-R	5G-R	1-2-3-4-5-6-7-8-9-10-11-12-13	NA	36-40-44-48-52-56-60-64-136-140-144-149-153-157-161-165
San Marino: SM	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	NA	36-40-44-48-52-56-60-64-100 -104-108-112-116-132-136-140
Slovak Republic: SK	2G-E	5G-E	1-2,-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112 -116-132-136-140
Slovenia: SI	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Spain: ES	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Sweden: SE	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
Switzerland: CH	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140	100-104-108-112-116-132-136-140
United Kingdom: GB	NA	NA	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165	100-104-108-112-116-120-124-128 -132-136-140-149-153-157-161-165
United States of America: US	2G-A	5G-B	1-2-3-4-5-6-7-8-9-10-11	NA	36-40-44-48-52-56-60-64-100-104-108-112-116-120-128-132-140-144-149-153 157-161-165
Vatican City: VA	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	NA	36-40-44-48-52-56-60-64-100-104-108-112-116-132-136-140

[7] From Cisco IOS XE 17.14.1, Israel has rejected the RoW domain standard and requires the usage of the following:

- Outdoor APs:
  - -I, effective July 2024

- Development of a Cisco Catalyst 9124 and 9163 domains that conform to Israel's outdoor AP requirements

- Indoor APs: Add Israel to the country list in the controller for -E domain APs
- Usage of -E on pre-RoW Wi-Fi 6 APs

Applicable post-RoW indoor APs: Cisco Catalyst 9136, 9162, 9164, and 9166 APs

Applicable pre-RoW indoor APs: Cisco Catalyst 9105, 9115, 9120, and 9130 APs

Restrictions on Regulatory Compliance Domain

- Cisco Catalyst 9124 AXE APs (9124AXE-F) are not supported in Indonesia. The AP radios are operationally down.

Countries Supporting 6-GHz Radio Band

The table below list the countries that support 802.11 6-GHz radio band:

The following APs support 6-GHz radio band:

- Cisco Catalyst 9136 Access Points
- Cisco Catalyst 9162 Series Access Points
- Cisco Catalyst 9164 Series Access Points
- Cisco Catalyst 9166 Series Access Points

From Cisco IOS XE Dublin 17.11.1, Albania, Iceland, Lichtenstein, Norway, and Switzerland are added to the list of countries that supports 6-GHz radio band.

From Cisco IOS XE Dublin 17.12.1, Australia, Brazil, Costa Rica, Honduras, Hong Kong, Japan, Jordan, Kenya, Malaysia, Morocco, New Zealand, Peru, Qatar, Saudi Arabia, and United Arab Emirates are added to the list of countries that supports 6-GHz radio band.

Note From Cisco IOS XE Dublin 17.12.2 onwards, 6-GHz radio band is not supported for Honduras country code (HN) in Cisco Catalyst 9136, 9162, 9164, and 9166 Series APs.

Table 19: Power Table and Supported Channels of Countries (6-GHz)

Country and Code	Outdoor Power Table 6-GHz	Supported Channels 6-GHz
Albania: AL	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49- 53-57-61-65-69-73-77-81-85-89-93

Country and Code	Outdoor Power Table 6-GHz	Supported Channels 6-GHz
Argentina: AR	6G -B1	1-5-9-13-17-21-25-29-33-37-41-45-49-53 -57-61-65-69-73-77-81-85-89 -93-97-101-105-109-113-117-121-125-129-133- 137-141-145-149-153-157-161-165-169-173 -177-181-185-189-193-197-201-205-209-213 -217-221-225-229-223
Austria: AT	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49- 53-57-61-65-69-73-77-81-85-89-93
Australia: AU	6G-Z	1-5-9-13-17-21-25-29-33-37-41-45-49- 53-57-61-65-69-73-77-81-85-89-93
Belgium: BE	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49- 53-57-61-65-69-73-77-81-85-89-93
Brazil: BR	6G-B1	1-5-9-13-17-21-25-29-33-37-41-45-49- 53-57-61-65-69-73-77-81-85-89-93-97-101-105-1 09-113-117–121-125-129-133-137-141-145-149- 153 157-161-165-169-173-177-181-185-189-193- 197-201-205-209-213–217-221-225-229-233
Bulgaria: BG	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49- 53-57-61-65-69-73-77-81-85-89-93
Canada: CA	6G-A	1-5-9-13-17-21-25-29-33-37-41-45-49- 53-57-61-65-69-73-77-81-85-89-93-97-101-105-1 09-113-117–121-125-129-133-137-141-145-149- 153 157-161-165-169-173-177-181-185-189-193- 197-201-205-209-213–217-221-225-229-233
Chile: CL	6G -B2	1-5-9-13-17-21-25-29-33-37-41-45-49-53- 57-61-65-69-73-77-81-85-89-93-97-101-105- 109-113-117-121-125-129-133-137-141-145- 149-153-157-161-165-169-173-177-181-185- 189-193-197-201-205-209-213-217-221-225-229-223

Country and Code	Outdoor Power Table 6-GHz	Supported Channels 6-GHz
Colombia: CO	6G-B1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117-121-125-129-133-137-141-145-149-153-157-161-165-169-173-177-181-185-189-193-197-201-205-209-213-217-221-225-229-223
Costa Rica: CR	6G-B1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117–121-125-129-133-137-141-145-149-153 157-161-165-169-173-177-181-185-189-193-197-201-205-209-213–217-221-225-229-233
Croatia: HR	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Cyprus: CY	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Czech Republic: CZ	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Denmark: DK	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Dominican Republic: DO	6G -B1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117-121-125-129-133-137-141-145-149-153-157-161-165-169-173-177-181-185-189-193-197-201-205-209-213-217-221-225-229-223
Estonia: EE	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Finland: FI	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
France: FR	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93

Country and Code	Outdoor Power Table 6-GHz	Supported Channels 6-GHz
Germany: DE	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Greece: GR	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Honduras: HN	6G-B1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117–121-125-129-133-137-141-145-149-153 157-161-165-169-173-177-181-185-189-193-197-201-205-209-213–217-221-225-229-233
Hong Kong: HK	6G-E2	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Hungary: HU	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Iceland: IS	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Ireland: IE	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Israel: IL[8]	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Italy: IT	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Japan: J4	6G-Q	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Jordan: JO	6G-E2	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Kenya: KN	6G-E2	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93

Country and Code	Outdoor Power Table 6-GHz	Supported Channels 6-GHz
Korea: KR	6G-K1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117–121-125-129-133-137-141-145-149-153 157-161-165-169-173-177-181-185-189-193-197-201-205-209-213–217-221-225-229
Latvia: LV	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Liechtenstein: LI	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Lithuania: LT	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Luxembourg: LU	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Malta: MT	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Malaysia: MY	6G-E2	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Mexico: MX	6G -B2	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117-121-125-129-133-137-141-145-149-153-157-161-165-169-173-177-181-185-189-193-197-201-205
Morocco: MO	6G-E2	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Netherlands: NL	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
New Zealand: NZ	6G-Z	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93

Country and Code	Outdoor Power Table 6-GHz	Supported Channels 6-GHz
Norway: NO	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Peru: PE	6G-B1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117-121-125-129-133-137-141-145-149-153-157-161-165-169-173-177-181-185-189-193-197-201-205-209-213-217-221-225-229-233
Poland: PL	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Portugal: PT	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Qatar: QA	6G-E2	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Romania: RO	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
San Marino: SM	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Saudi Arabia: SA	6G-B1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117-121-125-129-133-137-141-145-149-153-157-161-165-169-173-177-181-185-189-193-197-201-205-209-213-217-221-225-229-233
Singapore: SG	6G-Z	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Slovak Republic: SK	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Slovenia: SI	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
South Africa: ZA	6G-E2	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Spain: ES	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93

Country and Code	Outdoor Power Table 6-GHz	Supported Channels 6-GHz
Sweden: SE	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Switzerland: CH	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Thailand: TH	6G-Z	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
Turkey: TR	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
United Arab Emirates: AE	6G-E1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
United Kingdom: GB	6G-E1	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93
United States of America: US	6G-B	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93-97-101-105-109-113-117–121-125-129-133-137-141-145-149-153 157-161-165-169-173-177-181-185-189-193-197-201-205-209-213–217-221-225-229-233
Vatican City: VA	6G-E	1-5-9-13-17-21-25-29-33-37-41-45-49-53-57-61-65-69-73-77-81-85-89-93

[8] From Cisco IOS XE 17.14.1, Israel has rejected the RoW domain standard and requires the usage of the following:

- Outdoor APs:
  - -I, effective July 2024
  - Development of a Cisco Catalyst 9124 and 9163 domains that conform to Israel's outdoor AP requirements
- Indoor APs: Add Israel to the country list in the controller for -E domain APs
- Usage of -E on pre-RoW Wi-Fi 6 APs

Applicable post-RoW indoor APs: Cisco Catalyst 9136, 9162, 9164, and 9166 APs

Applicable pre-RoW indoor APs: Cisco Catalyst 9105, 9115, 9120, and 9130 APs

Rest of World Domain

Until Cisco IOS XE Bengaluru 17.5.1, APs used the global controller country list to configure and validate the country codes. From Cisco IOS XE Bengaluru 17.6.1 onwards, RoW domain support was added.

The following APs support RoW domain:

- Cisco Catalyst 9124AX outdoor Access Points
- Cisco Catalyst 9136 Access Points
- Cisco Catalyst 9164 Series Access Points
- Cisco Catalyst 9166 Series Access Points

From Cisco IOS XE Cupertino 17.9.1, the following countries are added to the RoW domain:

- Belarus
- Brunei
- Iraq
- Kazakhstan
- Kuwait
- Nigeria
- Pakistan
- Qatar
- Ukraine
- Uruguay

From Cisco IOS XE Dublin 17.11.1, the following countries are added to the RoW domain:

- Afghanistan
- Angola
- Bhutan
- Cambodia
- Democratic Republic of the Congo
- Ethiopia
- Georgia
- Honduras
- Ivory Coast
- Kosovo
- Laos
- Moldova

- Myanmar
- Nepal
- Nicaragua
- San Marino
- Sudan
- Vatican City State
- Yemen
- Zimbabwe

Note From Cisco IOS XE 17.14.1, Israel has rejected the RoW domain standard and requires the usage of the following:

- Outdoor APs:
  - -I, effective July 2024
  - Development of a Cisco Catalyst 9124 and 9163 domains that conform to Israel's outdoor AP requirements
- Indoor APs: Add Israel to the country list in the controller for -E domain APs
- Usage of -E on pre-RoW Wi-Fi 6 APs

Applicable post-RoW indoor APs: Cisco Catalyst 9136, 9162, 9164, and 9166 APs

Applicable pre-RoW indoor APs: Cisco Catalyst 9105, 9115, 9120, and 9130 APs

Table 20: Power Table and Supported Channels of Countries in RoW Domain

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4 GHz	Supported Channels 5 GHz
Afghanistan: AF	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116
Algeria: DZ	2G-E	5G-C1	1-2-3-4-5-6-7-8-9-10-11-12-13	52-56-60-64-100-104-108-112-116-132
Angola: AO	2G-E	—	1-2-3-4-5-6-7-8-9-10-11-12-13	—
Argentina: AR	2G-Z	5G-A1	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64-100-104-108-112-116-132-136-140 149-153-157-161-165

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4 GHz	Supported Channels 5 GHz
Bahamas: BS	2G-A	5G-B1	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60-64-149-153-157-161-165
Bahrain: BH	2G-E	5G-C1	1-2-3-4-5-6-7-8-9-10 11-12-13	149-153-157-161-165
Bangladesh: BD	2G-A	5G-A2	1-2-3-4-5-6-7-8-9-10- 11	149-153-157-161-165
Barbados: BB	2G-A	5G-B1	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64 149-153-157-161-165
Belarus: BY	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	132-136-140
Bhutan: BT	2G-E	—	1-2-3-4-5-6-7-8-9-10-11-12-13	—
Bolivia: BO	2G-A	5G-A10	1-2-3-4-5-6-7-8-9-10- 11	149-153-157-161-165
Bosnia: BA	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-0-11-12-13	100-104-108- 112-116-132-136-140
Brazil: BR	2G-Z	5G-Z1	1-2-3-4-5-6-7-8-9-10- 11-12-13	100- 104-112-116-120 124-128-132-136- 140-149-153-157- 161-165
Brunei: BN	2G-V1	5G-M3	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60-64- 116-120-124-128-132-136-140- 149-153-157-161-165
Cambodia: KH	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64
Cameroon: CM	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116-132-136-140
Chile: CL	2G-A	5G-A3	1-2-3-4-5-6-7-8-9-10- 11	52-56-60-64-100-104- 108-112-116-120-124-128-132- 136 140-149-153-157-161-165
China: CN	2G-E	5G-H1	1-2-3-4-5-6-7-8-9-10 11-12-13	149-153-157-161-165
Colombia: CO	2G-A	5G-B2	1-2-3- 4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64-100-104-108-112-116-120-124-128- 132 136-140-149-153-157-161-165

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4 GHz	Supported Channels 5 GHz
Cost Rica: CR	2G-A	5G-A4	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64- 100-104-108-112-116-120-124- 128-132-136-140-149-153-157-161-165
Democratic Republic of the Congo: CD	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64- 100-104-108-112-116
Dominican Republic: DO	2G-A	5G-A5	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-58-60-64- 100-104-108-112- 116-120-124-128- 132-136-140-149-153-157-161-165
Ecuador: EC	2G-A	5G-A4	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60-64- 100-104-108-112- 116-120-124-128- 132-136-140-149-153-157-161-165
Egypt: EG	2G-E	5G-C1	1-2-3-4-5-6-7-8-9-10- 11-12-13	36-40-44-48-52-56-60-64
El Salvador: SV	2G-A	5G-A	1-2-3-4-5-6-7-8-9-10- 11	52-56-60-64-149-153- 157-161-165
Ethiopia: ET	2G-E	—	1-2-3-4-5-6-7-8-9-10-11-12-13	—
Georgia: GE	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64- 100-104-108-112-116132- 136-140
Ghana: GH	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10- 11-12-13	100-104-108-112-116- 132-136-140
Gibraltar: GI	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
Honduras: HN	2G-A	5G-B2	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60-64- 100-104-108-112-116-120- 124-128-132-136-140-149-153 -157-161-165

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4 GHz	Supported Channels 5 GHz
Hong Kong: HK	2G-Z	5G-Z1	1-2-3-4-5-6-7-8-9-10- 11	100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165
India: IN	2G-Z	5G-D1	1-2-3-4-5-6-8-9-10-11	36-40-44-48-52-56-60- 100-104-108-112-116-124-128-132 136-140-144-153-157-161-165-169
Iraq: IQ	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116-132-136-140
Israel: IL	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	—
Ivory Coast: CI	2G-E	—	1-2-3-4-5-6-7-8-9-10-11-12-13	—
Jamaica: JM	2G-E	5G-Z	1-2-3-4-5-6-7-8-9-10- 11	52-56-60-64-100-104-108-112-116-120-124-128-132-136-140-153-161-165
Jordan: JO	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-52-56-60-64-100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165-169-172
Kazakhstan: KZ	2G-E	5G-E9	1-2-3-4-5-6-7-8-9-10- 11	100-104-108-112-116-132-136-140
Kenya: KE	2G-E	5G-E	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13	100-104-108-112-116-132-136-140
Korea: KR	2G-E	5G-K1	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60 64-100-104-108-112-116-120-124-128-132-136-140-149-153-157-161-165
Kosovo: XK	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64 -100-104-108-112-116-132-136-140
Kuwait: KW	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
Laos: LA	2G-E	—	1-2-3-4-5-6-7-8-9-10-11-12-13	—

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4 GHz	Supported Channels 5 GHz
Lebanon: LB	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
Macedonia: MK	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
Macao: MO	2G-V1	5G-M3	1- 2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60-64 116-120-124-128- 132-140-149-153 157-161-165
Malaysia: MY	2G-F	5G-C2	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116- 120-124-128-149-153- 157-161-165
Mexico: MX	2G-A1	5G-A6	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60- 64-149-153-157-161-165
Moldova: MD	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64- 100-104-108-112-116-132- 136-140
Mongolia: MN	2G-E1	5G-E6	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60-64 116-120-124-128- 132-140-149-153 157-161-165
Monaco: MC	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
Montenegro: ME	2G-E	5G-E	1-2-3-4-5- 6-7-8-9-10-11-12-13	100-104-108 112-116-132-136-140
Myanmar: MM	2G-E	—	1-2-3-4-5-6-7-8-9-10-11-12-13	—
Nepal: NP	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64- 100-104-108-112-116-132-136-140
Nicaragua: NI	2G-A	5G-A	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60-64- 100-104-108-112-116-132- 136-140-149-153-157-161-165
Nigeria: NG	2G-A1	5G-E5	1-2-3-4-5-6-7-8-9-10 11-12-13	52-56-60-64-149-153-157-161-165

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4 GHz	Supported Channels 5 GHz
Oman: OM	2G-E	5G-E	1-2-3-4-5-6 7-8-9-10-11-12-13	100-104-108- 112-116-132-136-140
Pakistan: PK	2G-A1	5G-E7	1-2-3-4-5-6-7-8-9-10- 11	149-153-157-161
Panama: PA	2G-A	5G-B2	1-2-3-4-5-6-7-8-9-10-11	36-40-44-48-52-56-60- 64-100-104-108-112- 116-120-124-128 132-136-140-149-153-157-161-165
Paraguay: PY	2G-A	5G-Z1	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60- 64-100-104-108-112- 116-120-124-128- 132-136-140-149-153-157-161-165
Peru: PE	2G-A	5G-A	1-2-3-4-5-6-7-8-9-10- 11	56-60-64-100-104-108 112-116-132-136-140- 149-153-157 161-165
Philippines: PH	2G-E	5G-A7	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64 100-104-108-112-116-120-128-136 140-149-153-157-161-165
Qatar : QA	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116 132-136-140
Rest of the World (Default)	2G-RW	5G-RW	1-2-3-4-5-6-7-8-9-10 11-12-13	—
Saudi Arabia: SA	2G-E	5G-M1	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116 120-124-128-132-136-140
Serbia: RS	2G-E	5G-E	1-2-3-4-5- 6-7- 8-9-10-11-12-13	100-104-108- 112-116-132-136-140
Singapore: SG	2G-V1	5G-M3	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60-64 116-120-124-128- 132-136-140-144 149-153-157-161-165
Slovak Republic: SK	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10 11-12-13	100-104-108-112-116- 132-136-140

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4 GHz	Supported Channels 5 GHz
South Africa: ZA	2G-E	5G-Z	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140-149-153-157-161-165
Sudan: SD	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-132-136-140
Taiwan: TW	2G-Z	5G-B	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64-100-104-108-112-116-120-128-132 140-144-149-153-157-161-165
Thailand: TH	2G-E	5G-M3	1-2-3-4-5-6-7-8-9-10 11-12-13	36-40-44-48-52-56-60- 64-116-120-124-128-132-136-140-149- 153-157-161-165
Trinidad: TI	2G-A1	5G-M2	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116 124-128-132-136-140
Tunisia: TN	2G-E	5G-C1	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
Turkey: TR	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
Ukraine: UA	2G-E	5G-E8	1-2-3-4-5-6-7-8-9-10-11-12-13	—
United Arab Emirates: AE	2G-E	5G-E	1-2-3-4-5- 6-7-8 9-10-11-12-13	100-104-108-112-116-132-136-140
United Kingdom: GB	2G-E	5G-E1	1-2-3-4-5-6-7-8-9-10-11-12-13	100-104-108-112-116-132-136-140
Uruguay: UY	2G-A	5G-A8	1-2-3-4-5-6-7-8-9-10-11	56-60-64-100-104-108-112-116-132-140-149-153-157-161-165
Venezuela: VE	2G-A	5G-A8	1-2-3-4-5-6-7-8-9-10- 11	36-40-44-48-52-56-60-64-149-153-157-161-165
Vietnam: VN	2G-V1	5G-M2	1-2-3-4-5-6-7-8-9-10-11-12-13	52-56-60-64-100-104-112-116-124-128-132-136-140-153- 157-161-165

Country and Code	Outdoor Power Table 2.4-GHz	Outdoor Power Table 5-GHz	Supported Channels 2.4 GHz	Supported Channels 5 GHz
Yemen: YE	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-132-136-140
Zimbabwe: ZW	2G-E	5G-E	1-2-3-4-5-6-7-8-9-10-11-12-13	36-40-44-48-52-56-60-64-100-104-108-112-116-132-136-140

Configuring Country Code for Rest of the World (CLI)

This configuration is mandatory for the RoW.

Follow the procedure given below to configure the country code.

Before you begin

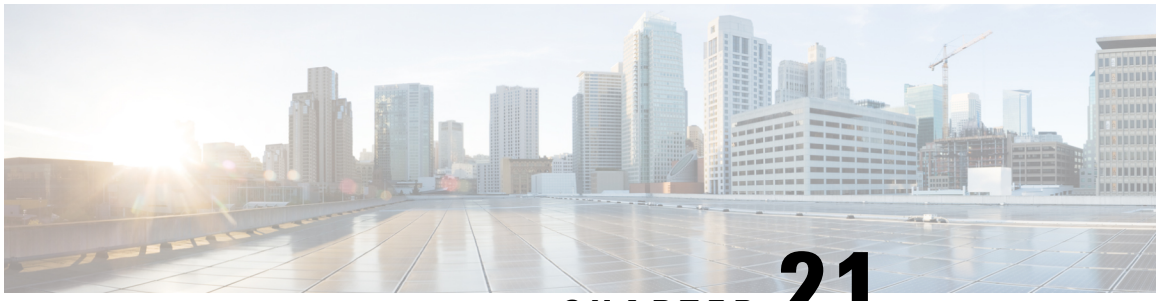
- Before configuring the country code in the AP profile, ensure that the country is present in the global country list. If the configured country code is not present in the global list, the AP retains the previous country code configuration. In addition, the misconfigured operation triggers a default flag and brings the radio operations down.
- If the configured country code does not match with the regulatory domain of one or more radio slots, the AP retains the previous country code configuration. In addition, the misconfigured operation triggers a default flag and brings the radio operations down.
- When a country is configured in an AP profile, a per AP country configuration on an AP mapped to that profile is not allowed.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile default-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** The Cisco Embedded Wireless Controller (EWC) supports only the default AP profile.
Step 3	**country** *code* **Example:**	Sets the country code. Use the **no** form of this command to delete the country code.

	Command or Action	Purpose
	`Device(config-ap-profile)# country IN`	**Note** From Cisco IOS XE Bengaluru 17.6.1, the **ap country** *code* command was modified. The **ap** keyword was removed. The modified command is **country** *code*.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

Step 5	**show ap profile name default-ap-profile detailed**
	Example:
	`Device# show ap profile name default-ap-profile detailed`
	
	`AP Profile Name : default-ap-profile`
	`Description : default ap profile`
	`.`
	`.`
	`.`
	`Country code : IN`
		Displays the AP country code for the AP join profile.
		If a country is not configured in the AP join profile, the country code will be displayed as "Not configured".
		The regulatory domain of RoW APs will be displayed as ROW.



CHAPTER 21

Access Points Modes

- Information about Sniffer, on page 308
- Information About XOR Radio Role Sniffer Support, on page 308
- Feature History for Sniffer Mode, on page 309
- Prerequisites for Sniffer, on page 309
- Restrictions on Sniffer, on page 309
- How to Configure Sniffer, on page 310
- Verifying Sniffer Configurations, on page 313
- Verifying XOR Radio Role Sniffer Configuration, on page 314
- Examples for Sniffer Configurations and Monitoring, on page 315
- Introduction to Monitor Mode, on page 315
- Enable Monitor Mode (GUI), on page 315
- Enable Monitor Mode (CLI), on page 316
- Feature History for Management Mode Migration in Cisco Catalyst Wireless 916X Access Points, on page 316
- Information About Management Mode Migration in Cisco Catalyst Wireless 916X Series Access Points, on page 317
- Regulatory Domain, on page 317
- Configuring Management Mode Migration (GUI), on page 321
- Configuring the AP Management Mode (CLI), on page 322
- Verifying the Management Mode Migration Details, on page 323
- Information About FlexConnect, on page 323
- Guidelines and Restrictions for FlexConnect, on page 327
- Configuring a Site Tag, on page 331
- Configuring a Policy Tag (CLI), on page 332
- Attaching a Policy Tag and a Site Tag to an Access Point (GUI), on page 333
- Attaching Policy Tag and Site Tag to an AP (CLI), on page 333
- Linking an ACL Policy to the Defined ACL (GUI), on page 334
- Applying ACLs on FlexConnect, on page 335
- Configuring FlexConnect, on page 336
- Flex AP Local Authentication (GUI), on page 342
- Flex AP Local Authentication (CLI), on page 343
- Flex AP Local Authentication with External Radius Server, on page 345
- Configuration Example: FlexConnect with Central and Local Authentication , on page 348
- NAT-PAT for FlexConnect, on page 348

• Split Tunneling for FlexConnect, on page 352
• VLAN-based Central Switching for FlexConnect, on page 359
• OfficeExtend Access Points for FlexConnect, on page 361
• Proxy ARP, on page 366
• Overlapping Client IP Address in Flex Deployment, on page 367
• Information About FlexConnect High Scale Mode, on page 370
• Flex Resilient with Flex and Bridge Mode Access Points, on page 371
• Feature History for OEAP Link Test, on page 376
• Information About OEAP Link Test, on page 377
• Configuring OEAP Link Test (CLI), on page 377
• Performing OEAP Link Test (GUI), on page 378
• Verifying OEAP Link Test, on page 378
• Feature History for Cisco OEAP Split Tunneling, on page 378
• Information About Cisco OEAP Split Tunneling, on page 379
• Prerequisites for Cisco OEAP Split Tunneling, on page 380
• Restrictions for Cisco OEAP Split Tunneling, on page 380
• Use Cases for Cisco OEAP Split Tunneling, on page 381
• Workflow to Configure Cisco OEAP Split Tunneling, on page 381
• Create an IP Address ACL (CLI), on page 381
• Create a URL ACL (CLI), on page 382
• Add an ACL to a FlexConnect Profile, on page 383
• Enable Split Tunnelling in a Policy Profile, on page 384
• Verifying the Cisco OEAP Split Tunnel Configuration, on page 384
• AP Survey Mode, on page 385

Information about Sniffer

The controller enables you to configure an access point as a network “sniffer”, which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on.

Sniffers allow you to monitor and record network activity, and detect problems.

The packet analyzer machine configured receives the 802.11 traffic encapsulated using the Airopeek protocol from the controller management IP address with source port UDP/5555 and destination UDP/5000.

You must use **Clear** in AP mode to return the AP back to client-serving mode, for example the local mode or FlexConnect mode depending on the remote site tag configuration.

Note It is recommended not to use the AP command to change the CAPWAP mode.

Information About XOR Radio Role Sniffer Support

The XOR radio in APs like Cisco 2800, 3800, 4800, and the 9100 series AP models support sniffer role in single radio interface.

The XOR radio offers the ability to operate as a single radio interface in many modes. This eliminates the need to place the entire AP into a mode. When this concept is applied to a single radio level, it is termed as role.

From this release onwards, Sniffer is the new supported role along with the Client Serving and Monitor roles.

Note The radio role is supported in Local and FlexConnect modes.

Feature History for Sniffer Mode

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 21: Feature History for Sniffer Mode

Release	Feature	Feature Information
Cisco IOS XE 17.8.1	XOR Radio Role Sniffer Support on the Access Point	The XOR radio in APs like Cisco 2800, 3800, 4800, and the 9100 series AP models support sniffer role in single radio interface.

Prerequisites for Sniffer

To perform sniffing, you need the following hardware and software:

- A dedicated access point—An access point configured as a sniffer cannot simultaneously provide wireless access service on the network. To avoid disrupting coverage, use an access point that is not part of your existing wireless network.
- A remote monitoring device—A computer capable of running the analyzer software.
- Software and supporting files, plug-ins, or adapters—Your analyzer software may require specialized files before you can successfully enable.

Restrictions on Sniffer

- Supported third-party network analyzer software applications are as follows:
  - Wildpackets Omnipeek or Airopeek
  - AirMagnet Enterprise Analyzer
  - Wireshark

- The latest version of Wireshark can decode the packets by going to the Analyze mode. Select **decode as**, and switch UDP5555 to decode as PEEKREMOTE..
- Sniffer mode is not supported when the controller L3 interface is the Wireless Management Interface (WMI).
- When an AP or a radio operates in the sniffer mode, irrespective of its current channel width settings, the AP sniffs or captures only on the primary channel.

Note As both Cisco Catalyst 9166I and 9166D APs have XOR radios, a Board Device File (BDF) has to be loaded to initialize radio 2 for the radios of these APs to work as expected. While the BDF is being loaded and for the file to be loaded correctly, the firmware has to be made non-operational and radios have to be reset. This operation of radio reset due to firmware being non-operational for the purposes of loading the BDFs is deliberate and is an expected behavior. This operation can be observed in both the controller and Cisco Catalyst Center. We recommend that you ignore the core dump that is generated due to this deliberate operation.

How to Configure Sniffer

Configuring an Access Point as Sniffer (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **General** tab, update the name of the AP. The AP name can be ASCII characters from 33 to 126, without leading and trailing spaces.

Step 3 Specify the physical location where the AP is present.

Step 4 Choose the **Admin Status** as **Enabled** if the AP is to be in enabled state.

Step 5 Choose the mode for the AP as *Sniffer*.

Step 6 In the **Tags** section, specify the appropriate policy, site, and RF tags that you created on the **Configuration** > **Tags & Profiles** > **Tags** page.

Note If the AP is in sniffer mode, you do not want to assign any tag.

Step 7 Click **Update & Apply to Device**.

Step 8 Choose the mode for the AP as **Clear** to return the AP back to the client-serving mode depending on the remote site tag configuration.

Note All the radios will be set to manual mode when you change the AP mode to Sniffer mode. Simultaneously, a warning message will be displayed informing you to convert the radio submode back to AUTO, if required, while changing the mode from Sniffer to other.

Configuring an Access Point as Sniffer (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode.
Step 2	**ap name** *ap-name* **mode sniffer** **Example:** `Device# ap name access1 mode sniffer`	Configures the access point as a sniffer. Where, *ap-name* is the name of the Cisco lightweight access point. Use the **no** form of this command to disable the access point as a sniffer.

Enabling or Disabling Sniffing on the Access Point (GUI)

Before you begin

Change the access point AP mode to sniffer mode.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **Access Points** page, click the AP name from the 6 GHz, 5 GHz, or 2.4 GHz list.

Step 3 In the **Role Assignment** section, select the **Assignment Method** as *Sniffer*.

Step 4 In the **Sniffer Channel Assignment** section, check the **Sniffer Channel Assignment** checkbox to enable.

Uncheck the checkbox to disable sniffing on the access point.

Step 5 From the **Sniff Channel** drop-down list, select the channel.

Note By default, the **Snif Channel** is set to *36* for the **5 GHz** and *1* for the **2.4 GHz**.

Step 6 Enter the IP address in the **Sniffer IP** field.

To validate the IP address, click **Update & Apply to Device**. If the IP address is valid, the **Sniffer IP Status** displays *Valid*.

Step 7 **Note** The section will be enabled for editing only if the **Assignment Method** is set to **Custom**.

In the **RF Channel Assignment** section, configure the following:

- From the **RF Channel Width** drop-down list, select the channel width.
- From the **Assignment Method** drop-down list, choose the the type of assignment.

Note If you choose Custom, you must select a channel width and specify an RF channel number to the access point radio.

Step 8 Click **Update & Apply to Device**.

Enabling or Disabling Sniffing on the Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**ap name** *ap-name* **sniff** {**dot11 6Ghz slot** *3 channel server-ip-address* | **dot11a** *channel server-ip-address* | **dot11b** *channel server-ip-address* | **dual-band** *channel server-ip-address*} **Example:** `Device# ap name access1 sniff dot11b 1 9.9.48.5`	Enables sniffing on the access point. • *channel* is the valid channel to be sniffed. For 802.11a, the range is 36 to 165. For 802.11b, the range is 1 to 14. For dot11 6Ghz, the range is between 1 and 233. • *server-ip-address* is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.
Step 3	**ap name** *ap-name* **no sniff** {**dot116Ghz** | **dot11a** | **dot11b** | **dual-band**} **Example:** `Device#ap name access1 no sniff dot116ghz`	Disables sniffing on the access point.

Configuring XOR Radio Role Sniffer Support on the Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**ap name** *ap-name* **dot11 {dual-band} shutdown** **Example:**	Shutdown the XOR radio.

	Command or Action	Purpose
	`Device# ap name AP687D.B45C.189C dot11 dual-band shutdown`	
Step 3	**ap name** *ap-name* **dot11 {dual-band} role manual {client-serving}** **Example:** `Device# ap name ap-name dot11 dual-band role manual client-serving`	Converts the XOR radio role to manual.
Step 4	**ap name** *ap-name* **dot11 {dual-band} band {5ghz | 24ghz}** **Example:** `Device# ap name  AP687D.B45C.189C dot11 dual-band band 5ghz`	Configures XOR radio to manually operate in a specific band.
Step 5	**ap name** *ap-name* **dot11 {dual-band} radio role manual sniffer channel** *channel-number* **ip** *ip-address* **Example:** `Device# ap name AP687D.B45C.189C dot11 dual-band radio role manual sniffer channel 100 ip 9.4.197.85`	Enables XOR radio role Sniffer support on AP from the controller. Where, • *ap-name* is the name of the Cisco lightweight access point. • *channel-number* is the channel number.
Step 6	**ap name** *ap-name* **no dot11 {dual-band} shutdown** **Example:** `Device# ap name AP687D.B45C.189C no dot11 dual-band shutdown`	Unshuts the XOR radio.
Step 7	**end** **Example:** `Device# end`	Returns to privileged EXEC mode. **Note** When configuring the radio to work as a Sniffer in the 5-GHz band, you will need to change the band of the radio manually as in **Step 4**.

Verifying Sniffer Configurations

Table 22: Commands for verifying sniffer configurations

Commands	Description
show ap name *ap-name* **config dot11** {**24ghz** | **5ghz** | **6ghz** | **dual-band**}	Displays the sniffing details.

Commands	Description
show ap name *ap-name* **config slot** *slot-ID*	Displays the sniffing configuration details. *slot-ID* ranges from 0 to 3. All access points have slot 0 and 1.

Verifying XOR Radio Role Sniffer Configuration

To verify the XOR radio role sniffer configuration for a given AP, use the following command:

```
Device# show ap name AP687D.B45C.189C config slot 0

Sniffing                                        : Enabled
Sniff Channel                                   : 6
Sniffer IP                                      : 9.4.197.85
Sniffer IP Status                               : Valid
ATF Mode                                        : Disable
ATE Optimization                                : N/A
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : information
Software Version                                : 17.9.0.18
Boot Version                                    : 1.1.2.4
Mini IOS Version                                : 0.0.0.0
Stats Reporting Period                          : 60
primary_discovery_timer                         : 120
LED State                                       : Enabled
LED Flash State                                 : Enabled
LED Flash Timer                                 : 0
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : PoE/Full Power
Number of Slots                                 : 4
AP Model                                        : C9136I-B
IOS Version                                     : 17.9.0.18
Reset Button                                    : Disabled
AP Serial Number                                : FOC25322JJZ
AP Certificate Type                             : Manufacturer Installed Certificate
AP Certificate Expiry-time                      : 08/09/2099 20:58:26
AP Certificate issuer common-name               : High Assurance SUDI CA
AP Certificate Policy                           : Default
AP CAPWAP-DTLS LSC Status
    Certificate status        : Not Available
AP 802.1x LSC Status
    Certificate status        : Not Available
AP User Name                                    : admin
AP 802.1X User Mode                             : Global
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 4 hours 20 minutes 55 seconds
AP CAPWAP Up Time                               : 4 hours 16 minutes 17 seconds
Join Date and Time                              : 01/19/2022 03:06:12

Attributes for Slot 0
  Radio Type                                    : 802.11ax - 2.4 GHz
  Radio Mode                                    : Sniffer
  Radio Role                                    : Sniffer
  Maximum client allowed                        : 400
  Radio Role Op                                 : Manual
```

```
Radio SubType                                : Main
Administrative State                         : Enabled
Operation State                              : Up
```

Examples for Sniffer Configurations and Monitoring

This example shows how to configure an access point as Sniffer:

```
Device# ap name access1 mode sniffer
```

This example shows how to enable sniffing on the access point:

```
Device# ap name access1 sniff dot11b 1 9.9.48.5
```

This example shows how to disable sniffing on the access point:

```
Device# ap name access1 no sniff dot11b
```

This example shows how to display the sniffing configuration details:

```
Device# show ap name access1 config dot11 24ghz
Device# show ap name access1 config slot 0
```

Introduction to Monitor Mode

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g/x access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

Note You can move an AP to a particular mode (sensor mode to local mode or flex mode) using the site tag with the corresponding mode. If the AP is not tagged to any mode, it will fall back to the mode specified in the default site tag.

You must use clear in AP mode to return the AP back to client-serving mode, for example the local mode or FlexConnect mode depending on the remote site tag configuration.

Enable Monitor Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Access Points** page, expand the **All Access Points** section and click the name of the AP to edit.

Step 3 In the **Edit AP** page, click the **General** tab and from the **AP Mode** drop-down list, choose **Monitor**.

Step 4 Click **Update & Apply to Device**.

Step 5 Choose the mode for the AP as **clear** to return the AP back to the client-serving mode depending on the remote site tag configuration.

Enable Monitor Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **mode monitor** **Example:** `Device# ap name 3602a mode monitor`	Enables monitor mode for the access point.
Step 2	**ap name** *ap-name* **monitor tracking-opt** **Example:** `Device# ap name 3602a monitor tracking-opt`	Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation.
Step 3	**ap name** *ap-name* **monitor-mode dot11b fast-channel** [*first-channel second-channel third-channel fourth-channel*] **Example:** `Device# ap name 3602a monitor dot11b 1 2 3 4`	Chooses up to four specific 802.11b channels to be scanned by the access point. In the United States, you can assign any value from 1 to 11 (inclusive) to the channel variable. Other countries support additional channels. You must assign at least one channel.
Step 4	**ap name** *ap-name* **dot11 6ghz slot** *3* **radio role manual monitor** **Example:** `Device# ap name cisco-ap dot11 6ghz slot 3 radio role manual monitor`	slot 3 radio role manual monitor Configures the 802.11 6-Ghz radio role manual monitor
Step 5	**show ap dot11 {24ghz | 5ghz | 6ghz} channel** **Example:** `Device# show ap dot11 5ghz channel`	Shows configuration and statistics of 802.11a or 802.11b or 6-GHz channel assignment.
Step 6	**show ap dot11 6ghz summary** **Example:** `Device# show ap dot11 6ghz summary`	Shows configuration and statistics summary of 6 the GHz band Cisco APs.

Feature History for Management Mode Migration in Cisco Catalyst Wireless 916X Access Points

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 23: Feature History for Management Mode Migration in Cisco Wireless Catalyst Wireless 916X Series Access Points

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	Management Mode Migration in Cisco Catalyst Wireless 916X Series Access Points	This feature allows you to convert the AP mode between DNA Management mode and Meraki Management mode, depending on your requirements. **Note** The document explains the conversion from DNA Management mode to Meraki Management mode and not vice versa.

Information About Management Mode Migration in Cisco Catalyst Wireless 916X Series Access Points

Cisco Catalyst Wireless 916x APs (CW9164I-x and CW9166I-x) support both cloud and controller architecture. You can migrate between cloud and controller deployments, depending on your requirements. The CW916x APs join and operate either in the DNA Management mode or in the Meraki Management mode. You can configure the management mode migration with the help of CLI commands in the privileged EXEC mode, at the AP level, and from the controller GUI.

CW916x APs support dual-band slot 3 radios, which in turn support both 6-GHz and 5-GHz bands.

Note The section explains the migration from DNA Management mode to the Meraki Management mode and not vice versa.

Regulatory Domain

For regulatory domain support, Cisco Catalyst 916x (CW916x) supports Rest of the World (RoW) and a few other fixed domains as shown here:

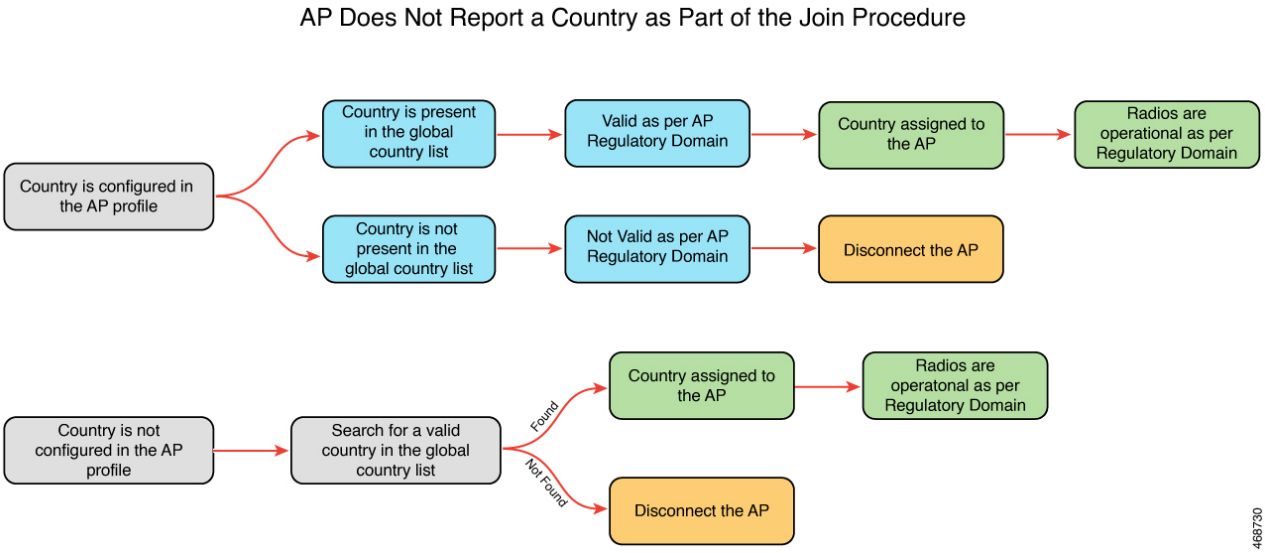
- -B
- -E
- -A
- -Z
- -Q
- -I
- -R

During the AP join flow, the regulatory domain details and the details of the country that is configured is passed on to the controller from the AP. The controller assigns or validates the right country of operation. After the country is validated based on the decision tree, the controller informs the AP about which country the AP should be configured with.

The following are the scenarios that determine the country that an AP should be configured with:

AP Configured with Non-RoW Regulatory Domain

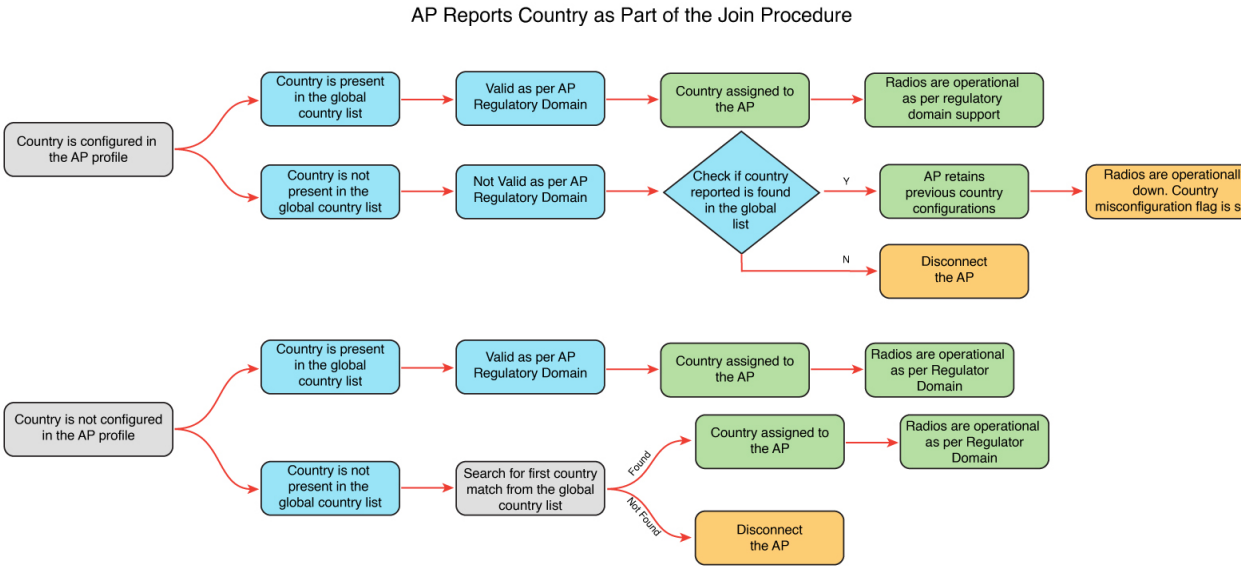
Case 1: AP does not report a country as part of the join procedure.



In the non-RoW regulatory domain, when an AP does not report a country as part of the join procedure, the following takes place:

- AP profile has a country configured.
  - If the country configured in the AP profile is present in the global country list, and is valid as per the AP regulatory domain, the country that is configured in the AP profile is assigned to the AP. Radios become operational as per the country or regulatory domain support.
  - If the country configured the AP profile is not present in the global country list, and is not valid as per the AP regulatory domain, the AP is disconnected.
- AP profile does not have a country configured. Find a valid country from the global country list (the first match), as per the AP regulatory domain.
  - If the country is found, the country is assigned to the AP and the radios become operational as per the country or regulatory domain support.
  - If the country is not found, the AP is disconnected.

Case 2: AP reports a country as part of the join procedure.



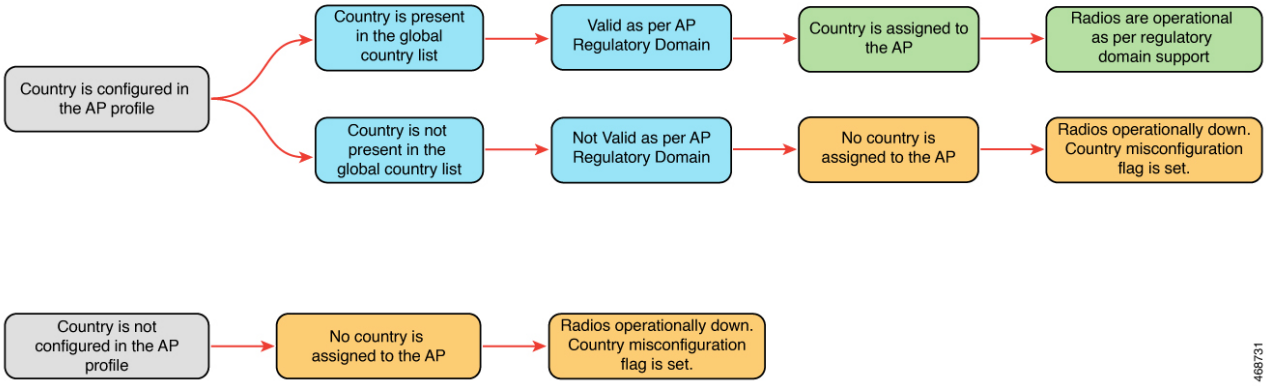
In the non-RoW regulatory domain, when an AP reports a country as part of the join procedure, the following takes place:

- The AP profile has a country configured.
  - If the country configured in the AP profile is present in the global country list, and it is valid as per the AP regulatory domain, the country that is configured in the AP profile is assigned to the AP. Radios become operational as per the country or regulatory domain support.
  - If the country configured in the AP profile is not present in the global country list, and is not valid as per the AP regulatory domain, check the global country list to confirm if the country is present in the list. If the country is present in the global list, the AP retains the previous country configuration and the radios are not operational with the country misconfiguration flag set. If the country is not located in the global list, the AP is disconnected.
- The AP profile does not have a country configured.
  - If the country reported by the AP is found in the global country list, and is valid as per the AP regulatory domain, the country is assigned to the AP and the radios become operational as per the country or regulatory domain support.
  - If the country is not present in the list, search for the first country match from the global list. If the country is found, the country is assigned to the AP and the radios become operational. If the country is not found, the AP is disconnected.

AP Configured with RoW Regulatory Domain

Case 1: The AP does not report a country as part of the join procedure.

AP Does Not Report a Country as Part of the Join Procedure

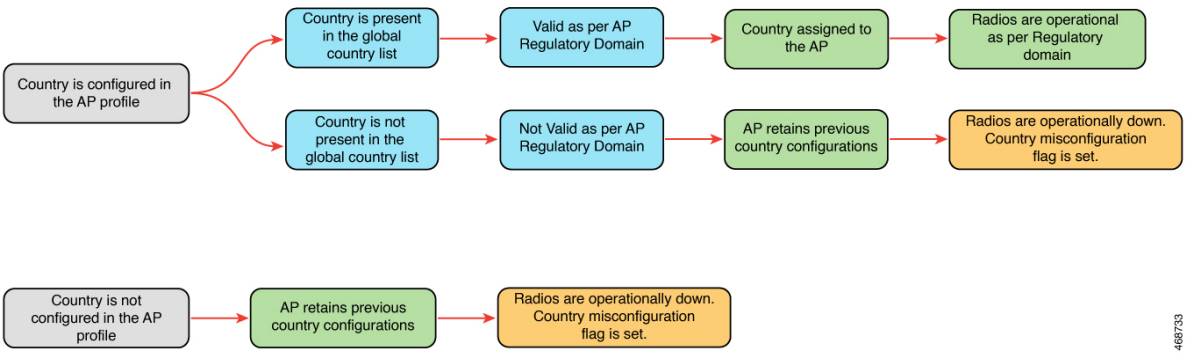


In the RoW regulatory domain, when an AP does not report a country as part of the join procedure, the following takes place:

- The AP profile has a country configured.
  - If the country configured in the AP profile is present in the global country list, and is valid as per the AP regulatory domain, country that is configured in the AP profile is assigned to the AP. Radios become operational as per the country or regulatory domain support.
  - If the country configured in the AP profile is not present in the global country list, and is not valid as per the AP regulatory domain, country is not assigned to the AP and radios are not operational, and the country misconfiguration flag is set.
- If the AP profile does not have a country configured, the country is not assigned to the AP and radios are not operational, and the country misconfiguration flag is set.

Case 2: The AP reports a country as part of the join procedure.

AP Reports a Country as Part of the Join Procedure



In the RoW regulatory domain, when an AP reports a country as part of the join procedure, the following takes place:

- The AP profile has a country configured.

- If the country configured in the AP profile is present in the global country list, and it is valid as per the AP regulatory domain, the country that is configured in the AP profile is assigned to the AP. Radios become operational as per the country or regulatory domain support.
- If the country configured in the AP profile is not present in the global country list, and is not valid as per the AP regulatory domain, the AP retains the previous country configuration and the radios are not operational with the country misconfiguration flag set.

- The AP retains the previous country configuration and the radios are not operational with the country misconfiguration flag set.

Configuring Management Mode Migration (GUI)

Before you begin

The country code must be configured on the AP profile. To configure the country code, navigate to **Configuration** > **Tags & Profiles** > **AP Join** page. Click an AP profile to edit. In the **General** tab, select the country code from the drop-down list.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Migrate to Meraki Management Mode**.

Step 2 Select the required APs by clicking on the check box(es), from the displayed APs.
The **Migrate to Meraki Management Mode** button is enabled.

Step 3 Click **Migrate to Meraki Management Mode** button to perform a validation check on the selected APs. If the validation check is successful, the **Next** button is enabled.

Step 4 Click **Next** to start the process.

Step 5 On the **Confirm Management Mode Migration** window, do the following:

a. Select the **Agree and continue** check box.

b. Click **Yes** to confirm.

The **Management Mode Migration Successful** section displays the APs that were migrated to the Meraki management mode. The **Management Mode Migration Failed** section displays the APs that were retained in DNA management mode.

Step 6 Click **Restart Workflow** to restart the workflow for APs that did not migrate from DNA management mode to Meraki management mode.

Exporting Meraki Management Mode-Migrated APs (GUI)

You can export the details about the Meraki management mode-migrated APs either from the **Change to Meraki Persona** tab after the workflow is completed or from the **Previously changed APs** tab.

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Wireless** > **Migrate to Meraki Management Mode**.	
Step 2	Click the **Export** button to export the list of APs.	
Step 3	Select whether you want to export only the current page or all pages. Click **Yes** to continue.	
Step 4	On the **Export** window, select the export method. The available options are:	• **Serial Number** • **JSON** • **Export to Meraki Dashboard** **Note** We recommend the Export to Meraki Dashboard option as you can directly export the migrated APs information into the Meraki Dashboard.
Step 5	Click **Copy** to copy the migrated APs. Click **Download** and save the file location.	

Configuring the AP Management Mode (CLI)

Before you begin

- Ensure that the AP is Meraki-capable to run any of the EXEC commands. To view the list of Meraki-capable APs, use the **show ap management-mode meraki capability summary** command.

Note If the country code is misconfigured, the change of management mode will not be allowed for any of the EXEC commands, except the **force** command.

If the regulatory domain is misconfigured for any slot, the change of management mode is not allowed for any of the EXEC commands, except the **force** command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter the password, if prompted.

	Command or Action	Purpose

Step 2	**ap name** *Cisco-AP-name* **management-mode meraki** [**force**] [**noprompt**]
	Example:
	`Device# ap name Cisco-AP-name management-mode meraki`
	`Device# ap name Cisco-AP-name management-mode meraki force`
	`Device# ap name Cisco-AP-name management-mode meraki noprompt`
	`Device# ap name Cisco-AP-name management-mode meraki force noprompt`
		Changes the AP management mode to Meraki.
		Here, **force** skips the validations at the controller and attempts Meraki management mode change at the AP.
		noprompt skips the user prompt for attempting AP management mode change.

Step 3	(Optional) **clear ap meraki stats** **Example:** `Device# clear ap meraki stats`	Clears the Meraki AP-related data.

Verifying the Management Mode Migration Details

To view the summary of the Meraki-capable AP information, run the following command:

```
Device# show ap management-mode meraki capability summary
AP Name                     AP Model             Radio MAC        MAC Address      AP Serial
 Number       Meraki Serial Number
-------------------------------------------------------------------------------------------
APXXXD.BXXX.1XXX          CW9162I            6XXd.bXXe.eXX0   6XXd.bXXe.eXX0    FOCXXXXXB90
            FOCXXXXXB90
```

To view the failure summary of the AP along with the migration attempt timestamp, run the following command:

```
Device# show ap management-mode meraki failure summary
AP Name              AP Model          Radio MAC        MAC Address      Conversion Attempt
        AP Serial Number       Meraki Serial Number   Reason Code
-------------------------------------------------------------------------------------------
APXXXD.BXXC.1        CW9162I          6XXd.bXXe.eXX0   6XXd.bXXe.eXX0   03/03/2022 17:17:42
 IST   FOCXXXXXB90            FOCXXXXXB90            Regulatory domain not set
```

To view the successful Meraki management mode migration attempts of all the APs, run the following command:

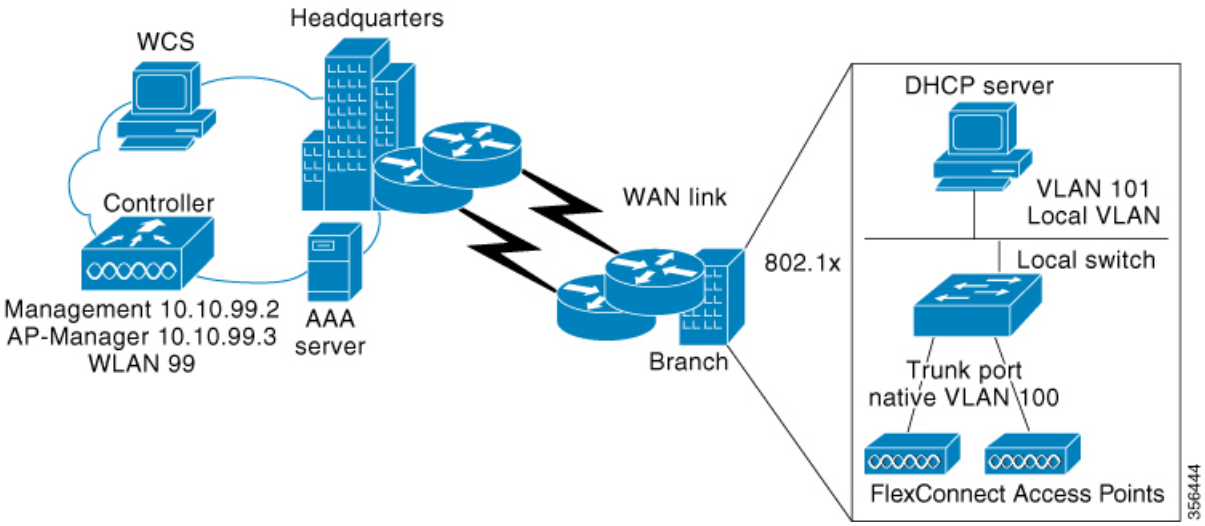
```
Device# show ap management-mode meraki change summary
AP Name                  AP Model          Radio MAC        MAC Address      Conversion
Timestamp       AP Serial Number        Meraki Serial Number
-------------------------------------------------------------------------------------------
APXXXX.3XXX.EXXX         CW9166I-B         1XXX.2XXX.1100   ccXX.3XXX.eXX0   05/02/2022
07:48:56 CST    KWC2XXXXX5G             Q5XX-4XXX-K7XX
```

Information About FlexConnect

FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points (AP) in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points

can also switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. FlexConnect access points support multiple SSIDs. In the connected mode, the FlexConnect access point can also perform local authentication.

Figure 16: FlexConnect Deployment



The controller software has a more robust fault tolerance methodology to FlexConnect access points. In previous releases, whenever a FlexConnect access point disassociates from a controller, it moves to the standalone mode. The clients that are centrally switched are disassociated. However, the FlexConnect access point continues to serve locally switched clients. When the FlexConnect access point rejoins the controller (or a standby controller), all the clients are disconnected and are authenticated again. This functionality has been enhanced and the connection between the clients and the FlexConnect access points are maintained intact and the clients experience seamless connectivity. When both the access point and the controller have the same configuration, the connection between the clients and APs is maintained.

After the client connection is established, the controller does not restore the original attributes of the client. The client username, current rate and supported rates, and listen interval values are reset to the default or new configured values only after the session timer expires.

The controller can send multicast packets in the form of unicast or multicast packets to an access point. In FlexConnect mode, an access point can receive only multicast packets.

In Cisco Catalyst 9800 Series Wireless Controller, you can define a flex connect site. A flex connect site can have a flex connect profile associate with it. You can have a maximum of 100 access points for each flex connect site.

FlexConnect access points support a 1-1 network address translation (NAT) configuration. They also support port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option. FlexConnect access points also support a many-to-one NAT or PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.

Workgroup bridges and Universal Workgroup bridges are supported on FlexConnect access points for locally switched clients.

FlexConnect supports IPv6 clients by bridging the traffic to local VLAN, similar to an IPv4 operation. FlexConnect supports Client Mobility for a group of up to 100 access points.

An access point does not have to reboot when moving from local mode to FlexConnect mode and vice-versa.

FlexConnect Authentication

When an access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image and configuration from the controller, and initializes the radio. It saves the downloaded configuration in nonvolatile memory for use in standalone mode.

Note Once the access point is rebooted after downloading the latest controller software, it must be converted to the FlexConnect mode.

Note 802.1X is not supported on the AUX port for Cisco Aironet 2700 series APs.

A FlexConnect access point can learn the controller IP address in one of these ways:

- If the access point has been assigned an IP address from a DHCP server, it can discover a controller through the regular CAPWAP or LWAPP discovery process.

Note OTAP is not supported.

- If the access point has been assigned a static IP address, it can discover a controller through any of the discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast, we recommend DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.
- If you want the access point to discover a controller from a remote network where CAPWAP or LWAPP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point CLI) the controller to which the access point is to connect.

Note The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

When a client associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

Note For the FlexConnect local switching, central authentication deployments, whenever passive client is enabled, the IP Learn timeout is disabled by default.

- central authentication, central switching—In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.

- central authentication, local switching—In this state, the controller handles client authentication, and the FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.
- local authentication, local switching—In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

  In connected mode, the access point provides minimal information about the locally authenticated client to the controller. The following information is not available to the controller:

  - Policy type
  - Access VLAN
  - VLAN name
  - Supported rates
  - Encryption cipher

  Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 576 bytes. In local authentication, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.
- Notes about local authentication are as follows:
  - Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.
  - Local RADIUS on the controller is not supported.
  - Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information.
- authentication down, switch down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected mode.
- authentication down, local switching—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a FlexConnect access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the “local authentication, local switching” state and continue new client authentications. This configuration is also correct for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or Cisco Centralized Key Management, but these authentication types require that an external RADIUS server be configured.

Other WLANs enter either the “authentication down, switching down” state (if the WLAN was configured for central switching) or the “authentication down, local switching” state (if the WLAN was configured for local switching).

When FlexConnect access points are connected to the controller (rather than in standalone mode), the controller uses its primary RADIUS servers and accesses them in the order specified on the RADIUS Authentication Servers page or in the **config radius auth add** CLI command (unless the server order is overridden for a

particular WLAN). However, to support 802.1X EAP authentication, FlexConnect access points in standalone mode need to have their own backup RADIUS server to authenticate clients.

Note A controller does not use a backup RADIUS server. The controller uses the backup RADIUS server in local authentication mode.

You can configure a backup RADIUS server for individual FlexConnect access points in standalone mode by using the controller CLI or for groups of FlexConnect access points in standalone mode by using either the GUI or CLI. A backup server configured for an individual access point overrides the backup RADIUS server configuration for a FlexConnect.

When web-authentication is used on FlexConnect access points at a remote site, the clients get the IP address from the remote local subnet. To resolve the initial URL request, the DNS is accessible through the subnet's default gateway. In order for the controller to intercept and redirect the DNS query return packets, these packets must reach the controller at the data center through a CAPWAP connection. During the web-authentication process, the FlexConnect access points allows only DNS and DHCP messages; the access points forward the DNS reply messages to the controller before web-authentication for the client is complete. After web-authentication for the client is complete, all the traffic is switched locally.

When a FlexConnect access point enters into a standalone mode, the following occurs:

- The access point checks whether it is able to reach the default gateway via ARP. If so, it will continue to try and reach the controller.

If the access point fails to establish the ARP, the following occurs:

- The access point attempts to discover for five times and if it still cannot find the controller, it tries to renew the DHCP on the ethernet interface to get a new DHCP IP.
- The access point will retry for five times, and if that fails, the access point will renew the IP address of the interface again, this will happen for three attempts.
- If the three attempts fail, the access point will fall back to the static IP and will reboot (only if the access point is configured with a static IP).
- Reboot is done to remove the possibility of any unknown error the access point configuration.

Once the access point reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and allows client connectivity again.

Guidelines and Restrictions for FlexConnect

- FlexConnect mode can support only 16 VLANs per AP.
- You can deploy a FlexConnect access point with either a static IP address or a DHCP address. In the context of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- FlexConnect supports up to 4 fragmented packets, or a minimum 576-byte maximum transmission unit (MTU) WAN link.

- Round-trip latency must not exceed 300 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. In scenarios where you cannot achieve the 300-ms round-trip latency, configure the access point to perform local authentication.
- Client connections are restored only for locally switched clients that are in the RUN state when the access point moves from standalone mode to connected mode. After the access point moves, the access point's radio is also reset.
- When multiple APs come from standalone mode to connected mode on FlexConnect and all the APs send the client entry in hybrid-REAP payload to the controller. In this scenario, the controller sends disassociation messages to the WLAN client. However, the WLAN client comes back successfully and joins the controller.
- When APs are in standalone mode, if a client roams to another AP, the source AP cannot determine whether the client has roamed or is just idle. So, the client entry at source AP will not be deleted until idle timeout.
- The configuration on the controller must be the same between the time the access point went into standalone mode and the time the access point came back to connected mode. Similarly, if the access point is falling back to a secondary or backup controller, the configuration between the primary and the secondary or backup controller must be the same.
- A newly connected access point cannot be booted in FlexConnect mode.
- FlexConnect mode requires that the client send traffic before learning the client's IPv6 address. Compared to in local mode where the controller learns the IPv6 address by snooping the packets during Neighbor Discovery to update the IPv6 address of the client.
- 802.11r fast transition roaming is not supported on APs operating in local authentication.
- The primary and secondary controllers for a FlexConnect access point must have the same configuration. Otherwise, the access point might lose its configuration, and certain features, such as WLAN overrides, VLANs, static channel number, and so on, might not operate correctly. In addition, make sure you duplicate the SSID of the FlexConnect access point and its index number on both controllers.
- If you configure a FlexConnect access point with a syslog server configured on the access point, after the access point is reloaded and the native VLAN other than 1, at the time of initialization, a few syslog packets from the access point are tagged with VLAN ID 1.
- MAC filtering is not supported on FlexConnect access points in standalone mode. However, MAC filtering is supported on FlexConnect access points in connected mode with local switching and central authentication. Also, Open SSID, MAC Filtering, and RADIUS NAC for a locally switched WLAN with FlexConnect access points is a valid configuration, where MAC is checked by Cisco ISE.
- FlexConnect does not display any IPv6 client addresses in the Client Detail window.
- FlexConnect access points with locally switched WLANs cannot perform IP source guard and prevent ARP spoofing. For centrally switched WLANs, the wireless controller performs IP source guard and ARP spoofing.
- To prevent ARP spoofing attacks in FlexConnect APs with local switching, we recommend that you use ARP inspection.
- Proxy ARP for VM clients (with any wireless host) does not work since the client includes many IP addresses for the same MAC. To avoid this issue, disable the ARP-caching option in the Flex profile.

- When you enable local switching on policy profile for FlexConnect APs, the APs perform local switching. However, for the APs in local mode, central switching is performed.

  In a scenario where the roaming of a client between FlexConnect mode AP and Local mode AP is not supported, the client may not get the correct IP address due to VLAN difference after the move. Also, L2 and L3 roaming between FlexConnect mode AP and Local mode AP are not supported.

  FlexConnect local switching is not supported on Cisco Aironet Cisco 1810T and 1815T (Teleworker) Access Points.

- Cisco Centralized Key Management (CCKM) is not supported in FlexConnect standalone mode. Hence, CCKM enabled client will not be able to connect when AP is in FlexConnect standalone mode.
- For Wi-Fi Protected Access Version 2 (WPA2) in FlexConnect standalone mode or local authentication in connected mode or Cisco Centralized Key Management fast roaming in connected mode, only Advanced Encryption Standard (AES) is supported.
- For Wi-Fi Protected Access (WPA) in FlexConnect standalone mode or local-auth in connected mode or Cisco Centralized Key Management fast-roaming in connected mode, only Temporal Key Integrity Protocol (TKIP) is supported.
- WPA2 with TKIP and WPA with AES is not supported in standalone mode, local-auth in connected mode, and Cisco Centralized Key Management fast-roaming in connected mode.
- WPA with TKIP is supported in non-FIPS mode.
- Only open, WPA (PSK and 802.1x), and WPA2 (AES) authentication is supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- Only 802.11r fast-transition roaming is supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- AVC on locally switched WLANs is supported on second-generation APs.
- Local authentication fallback is not supported when a user is not available in the external RADIUS server.
- For WLANs configured for FlexConnect APs in local switching and local authentication, synchronization of dot11 client information is supported.
- DNS override is not supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- The Cisco Aironet 1830 Series and 1850 Series APs do not support IPv6. However, a wireless client can pass IPv6 traffic across these APs.
- VLAN group is not supported in Flex mode under flex-profile.
- Configuring maximum number of allowed media streams on individual client or radio is not supported in FlexConnect mode.
- The WLAN client association limit will not work when the AP is in FlexConnect mode (connected or standalone) and is performing local switching and local authentication.
- A local switching client on FlexConnect mode will not get IP address for RLAN profile on the Cisco Aironet 1810 Series AP.
- Standard ACL is not supported on FlexConnect AP mode.
- IPv6 RADIUS Server is not configurable for FlexConnect APs. Only IPv4 configuration is supported.
- In Flex mode, IPv4 ACLs configured on WLAN gets pushed to AP but IPv6 ACLs does not.

- The client delete reason counters that are a part of the **show wireless stats client delete reasons** command, will be incremented only when the client record entry persists for join.

  For example, when an AP in the FlexConnect mode performs local authentication with ACL mismatch, then the AP deletes the client, and the controller does not create any client record.

- Cisco Centralized Key Management (CCKM) is supported in wave 1 APs in FlexConnect when you use local association.

- If the client roams from one AP to another and the roaming is successful, the following occurs:

  - The client does not send any traffic to the new AP.
  - The client's state is IP LEARN pending.
  - The client is deauthenticated after 180 seconds, if there is no traffic for the entire duration. In case the DHCP Required flag is set, the deauthentication occurs after 60 seconds.

- Using custom VLANs under the policy profile of the FlexConnect locally switched WLANs stops the SSID broadcast. In such scenarios, run the **shut** and **no shut** commands on the policy profile to start the SSID broadcast.

  SSIDs are broadcasted when you:

  - Perform VLAN name to id mapping under FlexConnect profile and map the custom VLAN name under the policy profile.
  - Use VLAN id or standard VLAN name, for example, VLANxxxx.

- In the FlexConnect mode, the group temporal key (GTK) timer is set to 3600 seconds by default on Cisco Wave 2 AP, and this value cannot be reconfigured.

- For Flex mode deployments, local association configured policy profiles are not supported at a given time on the WLAN. Only the local association command must be enabled.

- From Cisco IOS XE Amsterdam 17.1.1 release onwards, the police rate per client in the flex connect APs in the controller, is represented as **rate_out** for Ingress (input) and **rate_in** for Egress (output). To verify police rate on the flex AP, use the **show rate-limit client** command.

- FlexConnect APs do not forward the DHCP packets after Change of Authorization (CoA) and change of VLANs using 802.1X encryption. You must disconnect the client from the WLAN and reconnect the client to enable the client to get an IP address in the second VLAN.

- Cisco Wave 2 and Catalyst Wi-Fi6 APs in FlexConnect local switching mode do not support Layer2(PSK, 802.1X) + Layer3(LWA, CWA, redirection-based posturing) + Dynamic AAA override + NAC.

- In Cisco Catalyst 9136I APs, in FlexConnect local authentication, the ongoing session timeout for a client gets reset after every roam.

- Network access control (NAC) is not supported in FlexConnect local authentication.

- Multicast traffic on an AAA overridden VLAN is not supported. Using this configuration may result in potential traffic leaks between VLANs.

Configuring a Site Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site default-site-tag`	Configures site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	Maps a flex profile to a site tag.
Step 4	**ap-profile** *ap-profile* **Example:** `Device(config-site-tag)# ap-profile xyz-ap-profile`	Assigns an AP profile to the wireless site.
Step 5	**description** *site-tag-name* **Example:** `Device(config-site-tag)# description "default site tag"`	Adds a description for the site tag.
Step 6	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	Moves the access point to FlexConnect mode.
Step 7	**end** **Example:** `Device(config-site-tag)# end`	Saves the configuration, exits the configuration mode, and returns to privileged EXEC mode.
Step 8	**show wireless tag site summary** **Example:** `Device# show wireless tag site summary`	(Optional) Displays the summary of site tags.

Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy default-policy-tag`	Configures policy tag and enters policy tag configuration mode. **Note** When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.
Step 4	**description** *description* **Example:** `Device(config-policy-tag)# description "default-policy-tag"`	Adds a description to a policy tag.
Step 5	**remote-lan** *name* **policy** *profile-policy-name* {**ext-module**| **port-id** } **Example:** `Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2`	Maps a remote-LAN profile to a policy profile.
Step 6	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1`	Maps a policy profile to a WLAN profile. **Note** Ensure that the WLAN profile is not used by any other profiles. If the AP uses the default profile, ensure that the **no central switching** command is configured on other profiles.
Step 7	**end** **Example:** `Device(config-policy-tag)# end`	Exits policy tag configuration mode, and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	(Optional) Displays the configured policy tags. **Note** To view detailed information about a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Attaching a Policy Tag and a Site Tag to an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.
Step 2 Click the **Access Point** name.
Step 3 Go to the **Tags** section.
Step 4 Choose the **Policy Tag** from the **Policy** drop-down list.
Step 5 Choose the **Site Tag** from the **Site** drop-down list.
Step 6 Click **Update and Apply to Device**.

Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures a Cisco AP and enters AP profile configuration mode. **Note** The *mac-address* should be a wired mac address.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	Maps a policy tag to the AP.

	Command or Action	Purpose
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag rr-xyz-site`	Maps a site tag to the AP.
Step 5	**rf-tag** *rf-tag-name* **Example:** `Device(config-ap-tag)# rf-tag rf-tag1`	Associates the RF tag.
Step 6	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 7	**show ap tag summary** **Example:** `Device# show ap tag summary`	(Optional) Displays AP details and the tags associated to it.
Step 8	**show ap name** <*ap-name*> **tag info** **Example:** `Device# show ap name ap-name tag info`	(Optional) Displays the AP name with tag information.
Step 9	**show ap name** <*ap-name*> **tag detail** **Example:** `Device# show ap name ap-name tag detail`	(Optional) Displays the AP name with tag details.

Linking an ACL Policy to the Defined ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the Flex Profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 In the **Policy ACL** tab, click **Add**.

Step 5 Select the ACL from the **ACL Name** drop-down list and click **Save**.

Step 6 Click **Apply to Device**.

Applying ACLs on FlexConnect

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex Flex-profile-1`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**acl-policy** *acl-policy-name* **Example:** `Device(config-wireless-flex-profile)# acl-policy ACL1`	Configures an ACL policy. Access control lists (ACLs) perform packet filtering to control the movement of packets through a network.
Step 4	**exit** **Example:** `Device(config-wireless-flex-profile-acl)# exit`	Returns to wireless flex profile configuration mode.
Step 5	**native-vlan-id** **Example:** `Device(config-wireless-flex-profile)# native-vlan-id 25`	Configures native vlan-id information.
Step 6	**vlan** *vlan-name* **Example:** `Device(config-wireless-flex-profile)# vlan-name VLAN0169`	Configures a VLAN.
Step 7	**acl** *acl-name* **Example:** `Device(config-wireless-flex-profile-vlan)# acl ACL1`	Configures an ACL for the interface.
Step 8	**vlan-id***vlan-id* **Example:** `Device(config-wireless-flex-profile-vlan)# vlan-id 169`	Configures VLAN information.

Configuring FlexConnect

Configuring a Switch at a Remote Site

Procedure

Step 1 Attach the access point, which will be enabled for FlexConnect, to a trunk or access port on the switch.

Note The sample configuration in this procedure shows the FlexConnect access point connected to a trunk port on the switch.

Step 2 The following example configuration shows you how to configure a switch to support a FlexConnect access point.

In this sample configuration, the FlexConnect access point is connected to the trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers or resources on VLAN 101. A DHCP pool is created in the local switch for both the VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched.

```
.
.
.
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.201.224 255.255.255.224
   default-router 209.165.201.225
   dns-server 192.168.100.167
!
interface Gig1/0/1
 description Uplink port
 no switchport
 ip address 209.165.202.225 255.255.255.224
!
interface Gig1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 101
 switchport mode trunk
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
 ip address 209.165.201.225 255.255.255.224
end
!
.
```

.
.

Configuring the Controller for FlexConnect

You can configure the controller for FlexConnect in two environments:

- Centrally switched WLAN
- Locally switched WLAN

The controller configuration for FlexConnect consists of creating centrally switched and locally switched WLANs. This table shows three WLAN scenarios.

Table 24: WLAN Scenarios

WLAN	Security	Authentication	Switching	Interface Mapping (GUEST VLAN)
Employee	WPA1+WPA2	Central	Central	Management (centrally switched GUEST VLAN)
Employee-local	WPA1+WPA2 (PSK)	Local	Local	101 (locally switched GUEST VLAN)
Guest-central	Web authentication	Central	Central	Management (centrally switched GUEST VLAN)
Employee-local-auth	WPA1+WPA2	Local	Local	101 (locally switched VLAN)

Configuring Local Switching in FlexConnect Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click the name of a policy profile to edit it or click **Add** to create a new one.

Step 3 In the **Add/Edit Policy Profile** window that is displayed, uncheck the **Central Switching** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Local Switching in FlexConnect Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures the WLAN for local switching.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Central Switching in FlexConnect Mode (GUI)

Before you begin

Ensure that the policy profile is configured. If the policy profile is not configured, see *Configuring a Policy Profile (GUI)* section.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, select a policy.

Step 3 In the **Edit Policy Profile** window, in General Tab, use the slider to enable or disable **Central Switching**.

Step 4 Click **Update & Apply to Device**.

Configuring Central Switching in FlexConnect Mode

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures the WLAN for central switching.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an Access Point for FlexConnect

For more information, see *Configuring a Site Tag (CLI)* topic in New Configuration Model chapter.

Configuring an Access Point for Local Authentication on a WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 In the **Policy Profile** page, select a policy profile name. The **Edit Policy Profile** window is displayed.

Step 3 In the General tab, deselect **Central Authentication** check box.

Step 4 Click **Update & Apply to Device**.

Configuring an Access Point for Local Authentication on a WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**no central authentication** **Example:** `Device(config-wireless-policy)# no central authentication`	Configures the WLAN for local authentication.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Connecting Client Devices to WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created, as specified in the #unique_401 .

In the example scenarios (see #unique_401), there are three profiles on the client:

1. To connect to the *employee* WLAN, create a client profile that uses WPA or WPA2 with PEAP-MSCHAPV2 authentication. After the client is authenticated, the client is allotted an IP address by the management VLAN of the controller .
2. To connect to the *local-employee* WLAN, create a client profile that uses WPA or WPA2 authentication. After the client is authenticated, the client is allotted an IP address by VLAN 101 on the local switch.
3. To connect to the *guest-central* WLAN, create a client profile that uses open authentication. After the client is authenticated, the client is allocated an IP address by VLAN 101 on the network local to the access point. After the client connects, a local user can enter any HTTP address in the web browser. The user is automatically directed to the controller to complete the web authentication process. When the web login window appears, the user should enter the username and password.

Configuring FlexConnect Ethernet Fallback

Information About FlexConnect Ethernet Fallback

You can configure an AP to shut down its radio when the Ethernet link is not operational. When the Ethernet link comes back to operational state, you can configure the AP to set its radio back to operational state. This feature is independent of the AP being in connected or standalone mode. When the radios are shut down, the AP does not broadcast the WLANs, and therefore, the clients cannot connect to the AP, either through first association or through roaming.

Configuring FlexConnect Ethernet Fallback

Before you begin

This feature is not applicable to APs with multiple ports.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**fallback-radio-shut** **Example:** `Device(config-wireless-flex-profile)# fallback-radio-shut`	Enables radio interface shutdown.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 5	**show wireless profile flex detailed** *flex-profile-name* **Example:** `Device# show wireless profile flex detailed test`	(Optional) Displays detailed information about the selected profile.

Flex AP Local Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 In the **Flex** page, click the name of the **Flex Profile** or click **Add** to create a new one.

Step 3 In the **Add/Edit Flex Profile** window that is displayed, click the **Local Authentication** tab.

When local authentication and association is enabled in Access Point with Flex mode, the following occurs:

- AP handles the authentication.
- AP handles the rejection of client joins (in Mobility).

Note The controller does not increment statistics when AP rejects client association.

Step 4 Choose the server group from the **RADIUS Server Group** drop-down list.

Step 5 Use the **Local Accounting Radius Server Group** drop down to select the RADIUS server group.

Step 6 Check the **Local Client Roaming** check box to enable client roaming.

Step 7 Choose the profile from the **EAP Fast Profile** drop-down list.

Step 8 Choose to enable or disable the following:

- LEAP: Lightweight Extensible Authentication Protocol (LEAP) is an 802.1X authentication type for wireless LANs and supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys.
- PEAP: Protected Extensible Authentication Protocol (PEAP) is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- TLS: Transport Layer Security (TLS) is a cryptographic protocol that provide communications security over a computer network.
- RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

Step 9 In the **Users** section, click **Add**.

Step 10 Enter username and password details and click **Save**.

Step 11 Click **Save & Apply to Device**.

Flex AP Local Authentication (CLI)

Note The Cisco Catalyst 9800 Series Wireless Controller + FlexConnect local authentication + AP acting as RADIUS are not supported on Cisco COS and IOS APs.

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 2	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that all the session IDs information that is sent out from the RADIUS group for a given call are identical.
Step 3	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Enables system authorization control for the RADIUS group.
Step 4	**eap profile** *name* **Example:** `Device(config)# eap profile aplocal-test`	Creates an EAP profile.
Step 5	**method fast** **Example:** `Device(config-eap-profile)# method fast`	Configures the FAST method on the profile.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to configuration mode.
Step 7	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures the flex policy.
Step 8	**local-auth ap eap-fast** *name* **Example:** `Device(config-wireless-flex-profile)# local-auth ap eap-fast aplocal-test`	Configures EAP-FAST profile details.

	Command or Action	Purpose
Step 9	**local-auth ap leap** **Example:** `Device(config-wireless-flex-profile)# local-auth ap leap`	Configures the LEAP method.
Step 10	**local-auth ap peap** **Example:** `Device(config-wireless-flex-profile)# local-auth ap peap`	Configures the PEAP method.
Step 11	**local-auth ap username** *username* **Example:** `Device(config-wireless-flex-profile)# local-auth ap username test1 test1`	Configures username and password.
Step 12	**local-auth ap username** *username password* **Example:** `Device(config-wireless-flex-profile)# local-auth ap username test2 test2`	Configures another username and password.
Step 13	**exit** **Example:** `Device(config-wireless-flex-profile)# exit`	Returns to configuration mode.
Step 14	**wireless profile policy** *policy-profile* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures profile policy.
Step 15	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the policy profile.
Step 16	**no central authentication** **Example:** `Device(config)# no central authentication`	Disables central (controller) authentication.
Step 17	**vlan-id** *vlan-id* **Example:** `Device(config)# vlan-id 54`	Configures VLAN name or VLAN ID.
Step 18	**no shutdown** **Example:** `Device(config)# no shutdown`	Enables the configuration.

Flex AP Local Authentication with External Radius Server

In this mode, an access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 2	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that all the session ID's information that is sent out, from the RADIUS group for a given call are identical.
Step 3	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Enables the system authorization control for the RADIUS group.
Step 4	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name. **Note** To authenticate clients with freeradius over RADSEC, you should generate an RSA key longer than 1024 bit. Use the **crypto key generate rsa general-keys exportable label** *name* command to achieve this. Do not configure **key-wrap** option under the radius server and radius server group, as it may lead to clients getting stuck in authentication state.

Step 5	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* }
	Example:
	`Device(config-radius-server)# address ipv4 124.3.50.62 auth-port 1112 acct-port 1113`
	`Device(config-radius-server)# address ipv6 2001:DB8:0:20::15 auth-port 1812 acct-port 1813`
		Specifies the primary RADIUS server parameters.

	Command or Action	Purpose
Step 6	**key** *string* **Example:** `Device(config-radius-server)# key test123`	Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server. **Note** The maximum number of characters allowed for the shared secret is 63.
Step 7	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER2`	Specifies the RADIUS server name.

Step 8	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* }
	Example:
	`Device(config-radius-server)# address ipv4 124.3.52.62 auth-port 1112 acct-port 1113`
	`Device(config-radius-server)# address ipv6 2001:DB8:0:21::15 auth-port 1812 acct-port 1813`
		Specifies the secondary RADIUS server parameters.

Step 9	**key** *string* **Example:** `Device(config-radius-server)# key test113`	Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server.
Step 10	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to configuration mode.
Step 11	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius aaa_group_name`	Creates a RADIUS server group identification. **Note** *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.
Step 12	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name.
Step 13	**radius server** *server-name* **Example:** `Device(config-radius-server)# radius server Test-SERVER2`	Specifies the RADIUS server name.

	Command or Action	Purpose
Step 14	**exit** **Example:** `Device(config-radius-server)# exit`	Exit from RADIUS server configuration mode.
Step 15	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy.
Step 16	**local-auth radius-server-group** *server-group* **Example:** `Device(config-wireless-flex-profile)# local-auth radius-server-group aaa_group_name`	Configures the authentication server group name.
Step 17	**exit** **Example:** `Device(config-wireless-flex-profile)# exit`	Returns to configuration mode.
Step 18	**wireless profile policy** *policy-profile* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile.
Step 19	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables a policy profile.
Step 20	**no central authentication** **Example:** `Device(config-wireless-policy)# no central authentication`	Disables central (controller) authentication.
Step 21	**vlan-id** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan-id 54`	Configures a VLAN name or VLAN Id.
Step 22	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the configuration.

Configuration Example: FlexConnect with Central and Local Authentication

To see configuration example on how to configure a controller for FlexConnect central and local authentication, see the FlexConnect Configuration with Central and Local Authentication on Catalyst 9800 Wireless Controllers document.

NAT-PAT for FlexConnect

If you want to use a central DHCP server to service clients across remote sites, NAT-PAT should be enabled.

An AP translates the traffic coming from a client and replaces the client's IP address with its own IP address.

Note You must enable local switching, central DHCP, and DHCP required using the (**ipv4 dhcp required**) command to enable NAT and PAT.

Configuring NAT-PAT for a WLAN or a Remote LAN

Creating a WLAN

Follow the steps given here to create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Enters the WLAN configuration sub-mode. • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.

	Command or Action	Purpose
		Note If you have already configured WLAN, enter *wlan wlan-name* command.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Shut down the WLAN.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Wireless Profile Policy and NAT-PAT (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Click **Add**.
Step 3 In the **General** tab, enter the **Name** of the policy.
Step 4 Disable the **Central Switching** toggle button.
Step 5 Enable the **Central DHCP** toggle button.
Step 6 Enable the **Flex NAT/PAT** toggle button.
Step 7 In the **Advanced** tab, under the **DHCP** Settings, check the **IPv4 DHCP Required** check box.
Step 8 Click **Apply to Device**.

Configuring a Wireless Profile Policy and NAT-PAT

Follow the procedure given below to configure a wireless profile policy and NAT-PAT:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy nat-enabled-policy`	Configures the policy profile for NAT.

	Command or Action	Purpose
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures the WLAN for local switching.
Step 4	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures the DHCP parameters for WLAN.
Step 5	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Configures the central DHCP for locally switched clients.
Step 6	**flex nat-pat** **Example:** `Device(config-wireless-policy)# flex nat-pat`	Enables NAT-PAT.
Step 7	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.
Step 8	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Mapping a WLAN to a Policy Profile

Follow the procedure given below to map a WLAN to a policy profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy demo-tag`	Configures a policy tag and enters policy tag configuration mode.

	Command or Action	Purpose
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan wlan-demo policy nat-enabled-policy`	Maps a policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Site Tag

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	Moves an access point to FlexConnect mode.
Step 4	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching a Policy Tag and a Site Tag to an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the **Access Point** name.

Step 3 Go to the **Tags** section.

Step 4 Choose the **Policy Tag** from the **Policy** drop-down list.

Step 5 Choose the **Site Tag** from the **Site** drop-down list.

Step 6 Click **Update and Apply to Device**.

Attaching a Policy Tag and a Site Tag to an Access Point

Follow the procedure given below to attach a policy tag and a site tag to an access point:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters ap-tag configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag demo-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag flex-site`	Maps a site tag to the AP.
Step 5	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode.

Split Tunneling for FlexConnect

If a client that connects over a WAN link that is associated with a centrally switched WLAN has to send traffic to a device present in the local site, this traffic should be sent over CAPWAP to the controller, and the same traffic is sent back to the local site either over CAPWAP or with the help of some off-band connectivity.

This process consumes WAN link bandwidth unnecessarily. To avoid this, you can use the Split Tunneling feature, which allows the traffic sent by a client to be classified based on the packet contents. The matching packets are locally switched and the rest of the traffic is centrally switched. The traffic that is sent by the client that matches the IP address of the device present in the local site can be classified as locally switched traffic, and the rest of the traffic as centrally switched.

To configure local split tunneling on an AP, ensure that you have enabled DCHP Required on the policy profile using the (**ipv4 dhcp required**) command. This ensures that the client that is associating with the split WLAN does DHCP.

Note Apple iOS clients need option 6 (DNS) to be set in DHCP offer for split tunneling to work.

Note

- FlexConnect split tunneling (vlan-based central switching for FlexConnect) on auto-anchor deployment is not supported.
- Split tunneling does not work on RLAN clients. When the **split-tunnel** option is enabled on RLAN, traffic denied by the split tunnel ACL is not translated based on the IP address, instead the traffic is sent back to the controller through CAPWAP.
- URL filter must not be configured with wildcard URLs such as * and *.*

Configuring Split Tunneling for a WLAN or Remote LAN

Defining an Access Control List for Split Tunneling (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** dialog box, enter the **ACL Name**.

Step 4 Choose the ACL type from the **ACL Type** drop-down list.

Step 5 Under the **Rules** settings, enter the **Sequence** number and choose the **Action** as either **permit** or **deny**.

Step 6 Choose the required source type from the **Source Type** drop-down list.

a) If you choose the source type as **Host**, then you must enter the **Host Name/IP**.

b) If you choose the source type as **Network**, then you must specify the **Source IP** address and **Source Wildcard** mask.

Step 7 Check the **Log** check box if you want the logs.

Step 8 Click **Add**.

Step 9 Add the rest of the rules and click **Apply to Device**.

Defining an Access Control List for Split Tunneling

Follow the procedure given below to define an Access Control List (ACL) for split tunneling:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended split_mac_acl`	Defines an extended IPv4 access list using a name, and enters access-list configuration mode.
Step 3	**deny ip any host** *hostname* **Example:** `Device(config-ext-nacl)# deny ip any host 9.9.2.21`	Allows the traffic to switch centrally.
Step 4	**permit ip any any** **Example:** `Device(config-ext-nacl)# permit ip any any`	Allows the traffic to switch locally.
Step 5	**end** **Example:** `Device(config-ext-nacl)# end`	Exits configuration mode and returns to privileged EXEC mode.

Linking an ACL Policy to the Defined ACL

Follow the procedure given below to link an ACL policy to the defined ACL:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex flex-profile`	Configures the Flex profile and enters flex profile configuration mode.
Step 3	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy split_mac_acl`	Configures an ACL policy for the defined ACL.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Creating a WLAN

Follow the procedure given below to create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Specifies the WLAN name and ID: • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Wireless Profile Policy and a Split MAC ACL Name (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the policy.

Step 4 Enable the **Central Switching** toggle button.

Step 5 Enable the **Central DHCP** toggle button.

Step 6 In the **Advanced** tab, under the **DHCP** settings, check the **IPv4 DHCP Required** check box and enter the **DHCP Server IP Address**.

Step 7 Under the **WLAN Flex Policy** settings, choose the split MAC ACL from the **Split MAC ACL** drop-down list.

Step 8 Click **Apply to Device**.

Configuring a Wireless Profile Policy and a Split MAC ACL Name

Follow the procedure given below to configure a wireless profile policy and a split MAC ACL name:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy split-tunnel-enabled-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**flex split-mac-acl** *split-mac-acl-name* **Example:** `Device(config-wireless-policy)# flex split-mac-acl split_mac_acl`	Configures a split MAC ACL name. **Note** You should use the same ACL name for linking the flex and the policy profile.
Step 4	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures WLAN for central switching.
Step 5	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Enables central DHCP for centrally switched clients.
Step 6	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures the DHCP parameters for a WLAN.
Step 7	**ipv4 dhcp server** *ip_address* **Example:**	Configures the override IP address of the DHCP server.

	Command or Action	Purpose
	`Device(config-wireless-policy)# ipv4 dhcp server 9.1.0.100`	
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables a policy profile.

Mapping a WLAN to a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.
Step 2 Click **Add**.
Step 3 Enter the **Name** of the Tag Policy.
Step 4 Under **WLAN-POLICY Maps** tab, click **Add** .
Step 5 Choose the WLAN Profile from the **WLAN Profile** drop-down list.
Step 6 Choose the Policy Profile from the **Policy Profile** drop-down list.
Step 7 Click the **Tick** Icon .
Step 8 Click **Apply to Device**.

Mapping WLAN to a Policy Profile

Follow the procedure given below to map WLAN to a policy profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy split-tunnel-enabled-tag`	Configures a policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan wlan-demo policy split-tunnel-enabled-policy`	Maps a policy profile to a WLAN profile.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Site Tag

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	**Local site** is not configured on the site tag.
Step 4	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile flex-profile`	Configures a flex profile.
Step 5	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching a Policy Tag and Site Tag to an Access Point

Follow the procedure given below to attach a policy tag and site tag to an access point.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap** *ethernet-mac-address* **Example:** `Device(config)# ap 188b.9dbe.6eac`	Configures an AP and enters ap tag configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag split-tunnel-enabled-tag`	Maps a policy tag to an AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag flex-site`	Maps a site tag to an AP.
Step 5	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

VLAN-based Central Switching for FlexConnect

In FlexConnect local switching, if the VLAN definition is not available in an access point, the corresponding client does not pass traffic. This scenario is applicable when the AAA server returns the VLAN as part of client authentication.

When a WLAN is locally switched in flex and a VLAN is configured on the AP side, the traffic is switched locally. When a VLAN is not defined in an AP, the VLAN drops the packet.

When VLAN-based central switching is enabled, the corresponding AP tunnels the traffic back to the controller. The controller then forwards the traffic to its corresponding VLAN.

Note

- For VLAN-based central switching, ensure that VLAN is defined on the controller.
- VLAN-based central switching is not supported by mac filter.
- For local switching, ensure that VLAN is defined on the policy profile and FlexConnect profile.
- VLAN-based central switching with central web authentication enabled in Flex profile is not supported.

Configuring VLAN-based Central Switching (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the name of the policy profile.

Step 3 In the **Edit Policy Profile** window, perform these tasks:

a) Set **Central Switching** to **Disabled** state.

b) Set **Central DHCP** to **Disabled** state.

c) Set **Central Authentication** to **Enabled** state.

Step 4 Click the **Advanced** tab.

Step 5 Under **AAA Policy**, check the **Allow AAA Override** check box to enable AAA override.

Step 6 Under **WLAN Flex Policy**, check the **VLAN Central Switching** check box, to enable VLAN-based central switching on the policy profile.

Step 7 Click **Update & Apply to Device**.

Configuring VLAN-based Central Switching (CLI)

Follow the procedure given below to configure VLAN-based central switching.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a wireless policy profile.
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures a WLAN for local switching.
Step 4	**no central dhcp** **Example:** `Device(config-wireless-policy)# no central dhcp`	Configures local DHCP mode, where the DHCP is performed in an AP.
Step 5	**central authentication** **Example:** `Device(config-wireless-policy)# central authentication`	Configures a WLAN for central authentication.
Step 6	**aaa-override** **Example:**	Configures AAA policy override.

	Command or Action	Purpose
	`Device(config-wireless-policy)# aaa-override`	
Step 7	**flex vlan-central-switching** **Example:** `Device(config-wireless-policy)# flex vlan-central-switching`	Configures VLAN-based central switching.
Step 8	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.
Step 9	**show wireless profile policy detailed** *default-policy-profile* **Example:** `Device# show wireless profile policy detailed default-policy-profile`	(Optional) Displays detailed information of the policy profile.

OfficeExtend Access Points for FlexConnect

A Cisco OfficeExtend access point (OEAP) provides secure communications from a controller to a Cisco AP at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. A user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between an access point and the controller ensures that all communications have the highest level of security.

Note Preconfigure the controller IP for a zero-touch deployment with OEAP. All other home users can use the same access point to connect for home use by configuring the local SSID from AP.

Note In releases prior to Cisco IOS XE Amsterdam 17.3.2, when an AP is converted to OEAP, the local DHCP server on the AP is enabled by default. If the DHCP server on home router has a similar configuration, a network conflict occurs and AP will not be able to join back to the controller. In such a scenario, we recommend that you change the default DHCP server on the Cisco AP using OEAP GUI.

Note For OEAP, when configuration changes are made from the OEAP GUI to the following: Radio Status, Radio Interface Status, 802.11 n-mode, 802.11 ac-mode, Bandwidth, and Channel Selection (2.4 GHz or 5 GHz), CAPWAP should be restarted for the configuration sync to take place between the AP and the controller. During this interval, the AP GUI may not respond until the AP rejoins the controller. We recommend that you wait for the AP to rejoin the controller (for about 1-2 minutes), before you make further changes from the OEAP GUI.

Note In Cisco OfficeExtend access point (Cisco OEAP), if the OEAP local DHCP server is enabled and the user configures DNS IP from OEAP GUI, the wireless and wired clients connected to Cisco OEAP will receive that IP as DNS server IP in DHCP ACK.

Configuring OfficeExtend Access Points

Follow the procedure given below to configure OfficeExtend access points.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**office-extend** **Example:** `Device(config-wireless-flex-profile)# office-extend`	Enables the OfficeExtend AP mode for a FlexConnect AP.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode. **Note** After creating a flex profile, ensure that OEAP is in flex connect mode and mapped to its corresponding site tag. OfficeExtend is disabled by default. To clear the access point's configuration and return it to the factory-defaults, use the **clear ap config** *cisco-ap* command.

Disabling OfficeExtend Access Point

Follow the procedure given below to disable an OfficeExtend access point.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**no office-extend** **Example:** `Device(config-wireless-flex-profile)# no office-extend`	Disables OfficeExtend AP mode for a FlexConnect AP.
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Support for OEAP Personal SSID

Information About OEAP Personal SSID Support

The Cisco OfficeExtend Access Point supports personal SSID. This enables a local home client to use the same OfficeExtend Access Point for local networking and internet connectivity. With the help of the OEAP personal SSID feature, you can enable or disable personal SSID, enable or disable Datagram Transport Layer Security (DTLS) encryption between an access point and the controller, and enable rogue detection, using the knobs that are present on the AP profile page in the GUI. The local network access and DTLS encryption are enabled by default. The configurations described in this chapter is applicable for OEAP or for APs in the OEAP mode.

Configuring OEAP Personal SSID (GUI)

Procedure

Step 1 Choose **Configuration** > **AP Tags & Profiles** > **AP Join**.

The **AP Join Profile** section displays all the AP Join profiles.

Step 2 To edit the configuration details of an AP Join profile, select APs in the OEAP mode.
The **Edit AP Join Profile** window is displayed.

Step 3 In the **General** tab, under the **OfficeExtend AP Configuration** section, configure the following:

a) Check the **Local Access** check box to enable the local network. By default, **Local Access** is enabled. After the AP joins the controller using AP join profile where local access is enabled, the AP will not

broadcast the default personal SSID. Since the local access is enabled, you can login to the AP GUI and configure the personal SSID.

b) Check the **Link Encryption** check box to enable data DTLS. By default, **Link Encryption** is enabled.

c) Check the **Rogue Detection** check box to enable rogue detection. Rogue detection is disabled by default for OfficeExtend APs because these APs, deployed in a home environment, are likely to detect a large number of rogue devices.

Configuring OEAP Personal SSID (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile ap-profile`	Configures an AP profile and enters the AP profile configuration mode.
Step 3	**[no] oeap local-access** **Example:** `Device(config-ap-profile)# oeap local-access`	Enables the local access to AP. Local access consist of local AP GUI, LAN ports and personal SSID. The **no** form of this command disables the feature. If the local access is disabled, you will not be able to access the AP GUI, the local LAN port will be disabled, and personal SSID will not be broadcasted.
Step 4	**[no] oeap link-encryption** **Example:** `Device(config-ap-profile)# oeap link-encryption`	Enables DTLS encryption for OEAP APs or APs moving to the OEAP mode. The **no** form of this command disables the feature. This feature is enabled by default.
Step 5	**[no] oeap rogue-detection** **Example:** `Device(config-ap-profile)# no oeap rogue-detection`	Enables OEAP DTLS encryption in the AP profile configuration mode. This feature is disabled by default.

Viewing OEAP Personal SSID Configuration

To view the OEAP personal SSID configuration, run the following command.

```
Device# show ap profile name default-ap-profile detailed
.
.
.
OEAP Mode Config
Link Encryption : ENABLED
```

```
Rogue Detection : DISABLED
Local Access : ENABLED
```

Clearing Personal SSID from an OfficeExtend Access Point

To clear the personal SSID from an access point, run the following command:

ap name *Cisco_AP* **clear-personal-ssid**

Example: Viewing OfficeExtend Configuration

This example displays an OfficeExtend configuration:

```
Device# show ap config general

Cisco AP Name   : ap_name
================================================

Cisco AP Identifier                             : 70db.986d.a860
Country Code                                    : Multiple Countries : US,IN
Regulatory Domain Allowed by Country            : 802.11bg:-A   802.11a:-ABDN
AP Country Code                                 : US  - United States
AP Regulatory Domain
  Slot 0                                        : -A
  Slot 1                                        : -D
MAC Address                                     : 002c.c899.7b84
IP Address Configuration                        : DHCP
IP Address                                      : 9.9.48.51
IP Netmask                                      : 255.255.255.0
Gateway IP Address                              : 9.9.48.1
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Disabled
SSH State                                       : Disabled
Jumbo MTU Status                                : Disabled
Cisco AP Location                               : default location
Site Tag Name                                   : flex-site
RF Tag Name                                     : default-rf-tag
Policy Tag Name                                 : split-tunnel-enabled-tag
AP join Profile                                 : default-ap-profile
Primary Cisco Controller Name                   : uname-controller
Primary Cisco Controller IP Address             : 9.9.48.34
Secondary Cisco Controller Name                 : uname-controller1
Secondary Cisco Controller IP Address           : 0.0.0.0
Tertiary Cisco Controller Name                  : uname-ewlc2
Tertiary Cisco Controller IP Address            : 0.0.0.0
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : FlexConnect
AP Submode                                      : Not Configured
Office Extend Mode                              : Enabled
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : information
Software Version                                : 16.8.1.1
Boot Version                                    : 1.1.2.4
Mini IOS Version                                : 0.0.0.0
Stats Reporting Period                          : 0
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : PoE/Full Power (normal mode)
```

Proxy ARP

Proxy address resolution protocol (ARP) is the most common method for learning about MAC address through a proxy device. Enabling Proxy ARP known as ARP caching in Cisco Catalyst 9800 Series Wireless Controller means that the AP owning client is the destination of the ARP request, replies on behalf of that client and therefore does not send the ARP request to the client over the air. Access points not owning the destination client and receiving an ARP request through their wired connection will drop the ARP request. When the ARP caching is disabled, the APs bridge the ARP requests from wired-to-wireless and vice-versa increasing the air time usage and broadcasts over wireless.

The AP acts as an ARP proxy to respond to ARP requests on behalf of the wireless clients.

Enabling Proxy ARP for FlexConnect APs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the Flex Profile and check the **ARP Caching** check box. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Click **Apply to Device**.

Enabling Proxy ARP for FlexConnect APs

Follow the procedure given below to configure proxy ARP for FlexConnect APs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-policy* **Example:** `Device(config)# wireless profile flex flex-test`	Configures WLAN policy profile and enters wireless flex profile configuration mode.
Step 3	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	Enables ARP caching. **Note** Use the **no arp-caching** command to disable ARP caching.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config | section wireless profile flex** **Example:** `Device# show running-config | section wireless profile flex`	Displays ARP configuration information.
Step 6	**show wireless profile flex detailed** *flex-profile-name* **Example:** `Device# show wireless profile flex detailed flex-test`	(Optional) Displays detailed information of the flex profile.
Step 7	**show arp summary** **Example:** `Device# show arp summary`	(Optional) Displays ARP summary.

Overlapping Client IP Address in Flex Deployment

Overview of Overlapping Client IP Address in Flex Deployment

In flex deployments, you can use cookie cutter configuration across sites and branches which also includes local DHCP servers configured with the same subnet. In this topology, controllers detect multiple client sessions with the same IP as IP THEFT and clients are put in blocked list.

The Overlapping Client IP Address in Flex Deployment feature offers overlapping IP address across various flex sites and provides all the functionalities that are supported in flex deployments.

Enabling Overlapping Client IP Address in Flex Deployment (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex** and click **Add**.

Step 2 On the **Add Flex Profile** window and **General** tab.

Step 3 Check the **IP Overlap** check box to enable overlapping client IP Address in Flex deployment.

Step 4 Click **Apply to Device**.

Enabling Overlapping Client IP Address in Flex Deployment

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex flex1`	Configures a Flex profile and enters Flex profile configuration mode.
Step 3	[**no**] **ip overlap** **Example:** `Device(config-wireless-flex-profile)# [no] ip overlap`	Enables overlapping client IP address in flex deployment. **Note** By default, the configuration is disabled.

Verifying Overlapping Client IP Address in Flex Deployment (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **Clients**.

Step 2 Click the client in the table to view properties and statistics for each client.

Step 3 On the **Client** window and **General** tab, click **Client Statistics** tab to view the following details:

- Number of Bytes Received from Client
- Number of Bytes Sent to Client
- Number of Packets Received from Client
- Number of Packets Sent to Client
- Number of Policy Errors
- Radio Signal Strength Indicator
- Signal to Noise Ratio
- IP - Zone ID Mapping

Step 4 Click **OK**.

Verifying Overlapping Client IP Address in Flex Deployment

To verify if the overlapping client IP address in Flex deployment feature is enabled or not, use the following command:

```
Device# show wireless profile flex detailed flex1
Fallback Radio shut            : DISABLED
ARP caching                    : ENABLED
Efficient Image Upgrade        : ENABLED
OfficeExtend AP                : DISABLED
Join min latency               : DISABLED
IP overlap status              : DISABLED
```

To view additional details about the overlapping client IP address in Flex deployment feature, use the following command:

```
Device# show wireless device-tracking database ip

IP                                          ZONE-ID       STATE      DISCOVERY   MAC
-----------------------------------------------------------------------------------------------

  9.91.59.154                               0x00000002  Reachable   IPv4 Packet
6038.e0dc.3182
  1000:1:2:3:90d8:dd1a:11ab:23c0            0x00000002  Reachable   IPv6 Packet
58ef.680d.c6c3
  1000:1:2:3:f9b5:3074:d0da:f93b            0x00000002  Reachable   IPv6 Packet
58ef.680d.c6c3
  2001:9:3:59:90d8:dd1a:11ab:23c0           0x00000002  Reachable   IPv6 NDP
58ef.680d.c6c3
  2001:9:3:59:f9b5:3074:d0da:f93b           0x00000002  Reachable   IPv6 NDP
58ef.680d.c6c3
  fe80::f9b5:3074:d0da:f93b                 0x80000001  Reachable   IPv6 NDP
58ef.680d.c6c3
```

To view APs in various site tags, use the following command:

```
Device# show ap tag summary
Number of APs: 5

AP Name AP Mac Site Tag Name Policy Tag Name RF Tag Name Misconfigured Tag Source
-----------------------------------------------------------------------------------------------------------------------
AP3802 70b3.17f6.37aa flex_ip_overlap-site-tag-auto-3 flex_ip_overlap_policy_tag_1
default-rf-tag No Static
AP-9117AX 0cd0.f894.0f8c default-site-tag default-policy-tag default-rf-tag No Default
AP1852JJ9 38ed.18ca.2b48 flex_ip_overlap-site-tag-auto-2 flex_ip_overlap_policy_tag_2
default-rf-tag No Static
AP1852I 38ed.18cc.61c0 flex_ip_overlap-site-tag-auto-1 flex_ip_overlap_policy_tag_1
default-rf-tag No Static
AP1542JJ9 700f.6a84.1b30 flex_ip_overlap-site-tag-auto-2 flex_ip_overlap_policy_tag_2
default-rf-tag No Static
```

To view APs in FlexConnect mode, use the following command:

```
Device# show ap status
AP Name     Status      Mode        Country
-------------------------------------------------------------------------
AP3802      Disabled   FlexConnect   IN
AP1852I     Enabled    FlexConnect   US
AP-9117AX   Enabled    FlexConnect   IN
AP1542JJ9   Disabled   FlexConnect   US
AP1852JJ9   Enabled    FlexConnect   US
```

Troubleshooting Overlapping Client IP Address in Flex Deployment

To verify the WNCD instance for each of the APs, use the following command:

```
Device# show wireless loadbalance ap affinity wncd 0
AP Mac          Discovery Timestamp    Join Timestamp          Tag
------------------------------------------------------------------------------
0cd0.f894.0f8c   10/27/20 22:11:05    10/27/20 22:11:14    default-site-tag
38ed.18ca.2b48   10/27/20 22:06:09    10/27/20 22:06:19    flex_ip_overlap-site-tag-auto-2
700f.6a84.1b30   10/27/20 22:25:03    10/27/20 22:25:13    flex_ip_overlap-site-tag-auto-2
```

Information About FlexConnect High Scale Mode

This feature helps to scale up the FlexConnect site capacity to accommodate 300 APs and 3000 802.1x clients per site. The FlexConnect site capability is scaled up by using the Pairwise Master Key (PMK) option to skip Extensible Authentication Protocol (EAP) exchange while performing client roaming.

When a client associates with an AP under an 802.1x authentication architecture, an EAP exchange takes place, followed by a four-way handshake to verify the encryption keys. Using PMK caching, an AP can cache the PMK identifier of the EAP exchange, and for the subsequent client join. In PMK caching, the EAP exchange process is eliminated, and the authentication time process is decreased.

The PMK propagation feature is disabled by default. Until Cisco IOS XE Cupertino 17.7.1, the wireless controller used to push the PMK cache to every FlexConnect AP in the site. From Cisco IOS XE Cupertino 17.8.1 onwards, when PMK propagation is enabled, the controller pushes the PMK cache only to selective FlexConnect APs. These FlexConnect APs then forward the PMK identifier to the other FlexConnect APs within the same site.

Enabling PMK Propagation (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *test-flex-profile* **Example:** `Device(config)# wireless profile flex test-flex-profile`	Creates a FlexConnect profile.
Step 3	**pmk propagate** **Example:** `Device(config-wireless-flex-profile)# pmk propogate`	Propagates PMK information to the other APs in the site. **Note** The PMK propagation feature is disabled by default.

Examples

```
Device# configure terminal
Device(config)# wireless profile flex test-flex-profile
Device(config-wireless-flex-profile)# pmk propagate
```

Flex Resilient with Flex and Bridge Mode Access Points

Information About Flex Resilient with Flex and Bridge Mode Access Points

The Flex Resilient with Flex and Bridge Mode Access Points describe how to set up a controller with Flex+Bridge mode Access Points (APs) and Flex Resilient feature. The Flex Resilient feature works only in Flex+Bridge mode APs. The feature resides in Mesh link formed between RAP - MAP, once the link is UP and RAP loses connection to the CAPWAP controller, both RAP and MAP continue to bridge the traffic. A child Mesh AP (MAP) maintains its link to a parent AP and continues to bridge till the parent link is lost. A child MAP cannot establish a new parent or child link till it reconnects to the CAPWAP controller.

Note Existing wireless clients in locally switching WLAN can stay connected with their AP in this mode. No new or disconnected wireless client can associate to the Mesh AP in this mode. Client traffic in Flex+Bridge MAP is dropped at RAP switchport for the locally switched WLANs.

Configuring a Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click a **Flex Profile Name**. The **Edit Flex Profile** dialog box appears.

Step 3 Under the **General** tab, choose the **Flex Resilient** check box to enable the Flex Resilient feature.

Step 4 Under the **VLAN** tab, choose the required VLANs.

Step 5 (Optionally) Under the **Local Authentication** tab, choose the desired server group from the **Local Accounting RADIUS Server Group** drop-down list. Also, choose the **RADIUS** check box.

Step 6 Click **Update & Apply to Device**.

Configuring a Flex Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex new-flex-profile`	Configures a Flex profile and enters Flex profile configuration mode.
Step 3	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	Enables ARP caching.
Step 4	**description** *description* **Example:** `Device(config-wireless-flex-profile)# description "new flex profile"`	Enables default parameters for the Flex profile.
Step 5	**native-vlan-id** **Example:** `Device(config-wireless-flex-profile)# native-vlan-id 2660`	Configures native vlan-id information.
Step 6	**resilient** **Example:** `Device(config-wireless-flex-profile)# resilient`	Enables the resilient feature.
Step 7	**vlan-name** *vlan_name* **Example:** `Device(config-wireless-flex-profile)# vlan-name VLAN2659`	Configures VLAN name.
Step 8	**vlan-id** *vlan_id* **Example:** `Device(config-wireless-flex-profile)# vlan-id 2659`	Configures VLAN ID. The valid VLAN ID ranges from 1 to 4096.
Step 9	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuring a Site Tag (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site new-flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile new-flex-profile`	Configures a flex profile.
Step 4	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	**Local site** is not configured on the site tag.
Step 5	**site-tag** *site-tag-name* **Example:** `Device(config-site-tag)# site-tag new-flex-site`	Maps a site tag to an AP.
Step 6	**end** **Example:** `Device(config-site-tag)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuring a Mesh Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh Mesh_Profile`	Configures a Mesh profile and enters the Mesh profile configuration mode.

	Command or Action	Purpose
Step 3	**no ethernet-vlan-transparent** **Example:** `Device(config-wireless-profile-mesh)# no ethernet-vlan-transparent`	Disables VLAN transparency to ensure that the bridge is VLAN aware.
Step 4	**end** **Example:** `Device(config-wireless-profile-mesh)# end`	Exits configuration mode and returns to privileged EXEC mode.

Associating Wireless Mesh to an AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile new-ap-join-profile`	Configures the AP profile and enters AP profile configuration mode.
Step 3	**mesh-profile** *mesh-profile-name* **Example:** `Device(config-ap-profile)# mesh-profile Mesh_Profile`	Configures the Mesh profile in AP profile configuration mode.
Step 4	**ssh** **Example:** `Device(config-ap-profile)# ssh`	Configures the Secure Shell (SSH).
Step 5	**mgmtuser username** *username* **password** {**0** | **8**} *password* **Example:** `Device(config-ap-profile)# mgmtuser username Cisco password 0 Cisco secret 0 Cisco`	Specifies the AP management username and password for managing all of the access points configured to the controller. • **0**: Specifies an UNENCRYPTED password. • **8**: Specifies an AES encrypted password. **Note** While configuring an username, ensure that special characters are not used as it results in error with bad configuration.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Attaching Site Tag to an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters ap-tag configuration mode.
Step 3	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag new-flex-site`	Maps a site tag to the AP. **Note** Associating Site Tag causes the associated AP to reconnect.
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuring Switch Interface for APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**interface** *interface-id* **Example:** `Device(config)# interface <int-id>`	Enters the interface to be added to the VLAN.
Step 3	**switchport trunk native vlan** *vlan-id* **Example:**	Assigns the allowed VLAN ID to the port when it is in trunking mode.

	Command or Action	Purpose
	`Device(config-if)# switchport trunk native vlan 2660`	
Step 4	**switchport trunk allowed vlan** *vlan-id* **Example:** `Device(config-if)# switchport trunk allowed vlan 2659,2660`	Assigns the allowed VLAN ID to the port when it is in trunking mode.
Step 5	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Sets the trunking mode to trunk unconditionally. **Note** When the controller works as a host for spanning tree, ensure that you configure portfast trunk, using **spanning-tree portfast trunk** command, in the uplink switch to ensure faster convergence.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying Flex Resilient with Flex and Bridge Mode Access Points Configuration

To view the AP mode and model details, use the following command:

```
Device# show ap name <ap-name> config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-CAP3702I-A-K9
```

To view the MAP mode details, use the following command:

```
Device# show ap name MAP config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-CAP3702I-A-K9
```

To view the RAP mode details, use the following command:

```
Device# show ap name RAP config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-AP2702I-A-K9
```

To view if the Flex Profile - Resilient feature is enabled or not, use the following command:

```
Device# show  wireless profile flex detailed FLEX_TAG | inc resilient
Flex resilient                : ENABLED
```

Feature History for OEAP Link Test

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 25: Feature History for OEAP Link Test

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.5.1	OEAP Link Test	The Cisco OEAP Link Test feature allows you to determine the DTLS upload, link latency, and jitter of the link between an AP and the controller.

Information About OEAP Link Test

The Cisco OEAP Link Test feature allows you to determine the DTLS upload speed of the link between an AP and the controller. This feature helps in identifying network bottlenecks and reasons for functionality failures. You can determine the link latency by running a test on demand.

A link test is used to determine the quality of the link between the controller and an AP in OEAP mode. The AP sends synthetic packets to the controller and the controller echoes them back to the AP, which can then estimate the link quality.

Feature Scenarios

Cisco OfficeExtend Access Point (OEAP) users are complaining of poor performance when connected to a teleworker AP.

Use Cases

This feature allows OEAP network admins to troubleshoot low throughput from the Cisco Catalyst 9800 Controller GUI by running OEAP link test.

The OEAP link test provides DTLS upload speed, link latency, and link jitter, all of which help the network administrators to narrow down the problem.

Configuring OEAP Link Test (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **network-diagnostic** **Example:** `Device# ap name ap18 network-diagnostic`	Triggers network diagnostics on an OfficeExtend AP.

Performing OEAP Link Test (GUI)

Procedure

Step 1 Choose **Monitoring > Wireless > AP Statistics**.

In the list of APs, a **Link Test** icon is displayed in the **AP Name** column for OEAP-capable APs.

Note The **Link Test** icon is displayed only if an AP is OEAP capable and is configured to operate as OEAP.

Step 2 Click **Link Test**.

A link test is run and the results are shown.

Verifying OEAP Link Test

The following example shows how to verify network diagnostics information:

```
Device# show FlexConnect office-extend diagnostics

Summary of OfficeExtend AP Link Latency

CAPWAP Latency Heartbeat

Current: current latency (ms)
Min: minimum latency (ms)
Max: maximum latency (ms)

Link Test

Upload: DTLS Upload (Mbps)
Latency: DTLS Link Latency (ms)
Jitter: DTLS Link Jitter (ms)

AP Name Last Latency Heartbeat from AP Current Max Min Last Link Test Run Upload Latency
Jitter
-----------------------------------------------------------------------------------------------
ap-18   1 minute 1 second              0       0   0   12/04/20 09:19:48  8      2
 0
```

Feature History for Cisco OEAP Split Tunneling

This table provides release and related information for the feature explained in this module.

This feature is available in all the releases subsequent to the one in which it is introduced in, unless noted otherwise.

Table 26: Feature History for Cisco OEAP Split Tunneling

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	IPv6 Support	IPv6 addressing is supported on the Cisco OEAP Split Tunneling feature.
Cisco IOS XE Cupertino 17.7.1	Cisco OEAP Split Tunneling	The Split Tunneling feature in Cisco OfficeExtend Access Point (OEAP) provides a mechanism to classify client traffic, based on packet content, using access control lists (ACLs).

Information About Cisco OEAP Split Tunneling

The global pandemic has redefined the way people interact and work. The workplace has shifted from office cubicles to home desks, which requires applications that enable seamless collaboration among the workforce. For home-based workers, access to business services must be reliable, consistent, and secure. It should provide an experience that is similar to the office facility. Routing all of the traffic through the corporate network using traditional VPNs increases the traffic volume, slows down access to resources, and negatively impacts the remote user experience.

Cisco OEAP provides secure communications from a controller to an access point (AP) at a remote location, seamlessly extending the corporate WLAN over the internet to an employee's residence. Cisco OEAP provides segmentation of home and corporate traffic using the Split Tunnelling feature, which allows for home device connectivity without security risks to corporate policy.

Split tunnelling classifies the traffic sent by a client, based on packet content, using ACLs. Matching packets are switched locally from Cisco OEAP, and other packets are centrally switched over CAPWAP. Clients on a corporate SSID can talk to devices on a local network (printers, wireless devices on a personal SSID, and so on) directly without consuming WAN bandwidth, by sending packets over CAPWAP.

Traffic to Software as a Service (Saas) applications such as Cisco WebEx, Microsoft SharePoint, Microsoft Office365, Box, Dropbox, and so on that is required as part of the work routine, need not go through the corporate network, by using the Split Tunnelling feature.

The Cisco OEAP advertises two SSIDs, one corporate and one personal. Corporate SSID clients obtain their IP address from the central DHCP server in the corporate network. If split tunneling is enabled and a client wants to access a device in the home network, the AP performs NAT (PAT) translation between the wireless client corporate network subnet and the home network where the AP is located.

The personal SSID is configurable by a Cisco OEAP user. Clients will either get their IP address from the home router (when the AP personal SSID firewall is disabled) or from the internal AP DHCP server (when the AP personal SSID firewall is enabled). In the latter scenario, if the clients want to reach the home network devices, the AP perform sNAT (PAT) translation between the wireless client's internal network and the home network where the AP is located.

IPv6 Address Support

From Cisco IOS XE Cupertino 17.8.1, IPv6 addressing is supported. You can disable IPv6 addressing only by disabling the feature.

Note The end-to-end network should support IPv6, that is, both the corporate network (controller, corporate gateway, and so on) and the home network (wireless clients, home router, and so on) should support IPv6.

Prerequisites for Cisco OEAP Split Tunneling

- Cisco Wave 2 APs or Cisco Catalyst 9100AX Series Access Points
- URL filter list that matches the ACL name configured in split tunneling

Restrictions for Cisco OEAP Split Tunneling

- Cisco OEAPs are not supported when Cisco Embedded Wireless Controller on Catalyst Access Points (EWC) is used as a controller.
- Mesh topology is not supported.
- Clients connected on personal SSID or on home network (AP native VLAN) cannot discover devices on the corporate network.
- Split tunnelling is not supported in standalone mode.
- URL split tunnelling supports only up to 512 URLs.
- Action (deny or permit) can be specified only on the URL filter list, not for each individual entry.
- If URL-based ACL contains wild-card URLs, a maximum of 10 URLs are supported.
- The amount of snooped DNS IP addresses is limited as follows:
  - An AP can snoop 4095 IP addresses per DNS response, if IP addresses are less than 150,000.
  - An AP can snoop 10 IP addresses per DNS response, if IP addresses are between 150,000 and 200,000.
  - An AP can snoop five IP addresses per DNS response, if IP addresses are between 200,000 and 250,000.
  - An AP can snoop one IP address per DNS response, if IP addresses are greater than 250,000.
- A maximum of 128 IP address ACE (rules) can be used in the IP ACL for split tunnelling.
- URL-based split tunnelling only works with IPv4 addresses.
- The following restrictions are specific to IPv6 addressing
  - Multihoming (multiple router advertisement prefixes) is not supported (If a home network receives multiple prefixes, the one used by the AP that is connected to the controller is used.)
  - Roaming is not supported.
  - Filtering is not supported on the upstream traffic towards the wireless client.

- Split tunneling is disabled for clients with duplicate IPv6 addresses. Traffic for these clients is forwarded centrally to the controller.
- DHCPv6 prefix delegation is not supported for wireless clients.
- If the corporate prefix length is smaller than the home prefix length, split tunneling for a particular client is disabled.

Use Cases for Cisco OEAP Split Tunneling

Before Release 17.7.1, split tunneling used IP ACLs. This meant that cloud services such as Cisco Webex were accessed directly without going through the corporate network. The network administrator maintained the list of IP addresses that Cisco Webex used, which was a daunting task. From Release 17.7.1, using the Cisco OEAP Split Tunneling feature, the network administrator needs to provide only the DNS names that Cisco Webex uses. The AP ensures that traffic from these DNS names is routed directly to the internet without using the corporate network.

Workflow to Configure Cisco OEAP Split Tunneling

1. Create an IP address ACL or URL ACL
2. Add ACL to FlexConnect Profile
3. Enable Split Tunnelling on Policy Profile
4. Verify the Configuration

Create an IP Address ACL (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended vlan_oeap`	Defines an extended IPv4 access list using a name. **Note** IP ACL can be used to define a default action if there is no match in the URL ACL.
Step 3	*seq-num* **deny ip any host** *hostname* **Example:**	Denies IP traffic from any host.

	Command or Action	Purpose
	`Device(config-ext-nacl)# 10 deny ip any 10.10.0.0 0.0.255.255`	
Step 4	*seq-num* **permit ip any any** *hostname* **Example:** `Device(config-ext-nacl)# 20 permit ip any any`	Permits IP traffic from any source or destination host.
Step 5	**end** **Example:** `Device(config-ext-nacl)# end`	Exits configuration mode and returns to privileged EXEC mode.

Create a URL ACL (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter list** *list-name* **Example:** `Device(config)# urlfilter list vlan_oeap`	Configures the URL filter list. The list name must not exceed 32 alphanumeric characters.
Step 3	**action permit** **Example:** `Device(config-urlfilter-params)# action permit`	Configures the action: Permit (traffic is allowed directly on the home network) or Deny (traffic is directed to the corporate network).
Step 4	**filter-type post-authentication** **Example:** `Device(config-urlfilter-params)# filter-type post-authentication`	Configures the URL list as post authentication filter.
Step 5	**url** *url-name* **Example:** `Device(config-urlfilter-params)# url wiki.cisco.com`	Configures a URL.
Step 6	**url** *url-name* **Example:** `Device(config-urlfilter-params)# url example.com`	(Optional) Configures a URL. Use this option when you want to add multiple URLs.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-urlfilter-params)# end`	Exits configuration mode and returns to privileged EXEC mode.

Add an ACL to a FlexConnect Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures a FlexConnext profile.
Step 3	**acl-policy** *acl-policy-name* **Example:** `Device(config-wireless-flex-profile)# acl-policy vlan_oeap`	Configures an ACL policy.
Step 4	**urlfilter list** *url-filter* **Example:** `Device(config-wireless-flex-profile-acl)# urlfilter list vlan_oeap`	Configures a URL filter list.
Step 5	**exit** **Example:** `Device(config-wireless-flex-profile-acl)# exit`	Returns to FlexConnect profile configuration mode..
Step 6	**office-extend** **Example:** `Device(config-wireless-flex-profile)# office-extend`	Enables the OEAP mode for a FlexConnect AP.
Step 7	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Enable Split Tunnelling in a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures a FlexConnect profile.
Step 3	**no central association** **Example:** `Device(config-wireless-flex-profile)# no central association`	Disables central association and enables local association for locally switched clients.
Step 4	**flex split-mac-acl** *split-mac-acl-name* **Example:** `Device(config-wireless-flex-profile)# flex split-mac-acl vlan_oeap`	Configures a split MAC ACL name. **Note** Ensure that you use the same *acl-policy-name* in the FlexConnect profile.
Step 5	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying the Cisco OEAP Split Tunnel Configuration

To verify the split tunneling DNS ACLs per wireless client on the AP side, use the following command:

```
Device# show split-tunnel client 00:11:22:33:44:55 access-list

Split tunnel ACLs for Client: 00:11:22:33:44:55

IP ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
             1          242           3       768

URL ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
             3          778           0         0

Resolved IPs for Client: 00:11:22:33:44:55 for Split tunnel
```

```
HIT-COUNT       URL             ACTION  IP-LIST

1               base1.com       deny.   20.0.1.1
                                        20.0.1.10

2               base2.com       deny.   20.0.1.2

3               base3.com       deny.   20.0.1.3
```

To verify the current binding between a WLAN and an ACL, use the following command:

```
Device# show split-tunnel mapping

VAP-Id       ACL Name
    0        SplitTunnelACL
```

To verify the content of the current URL ACL, use the following command:

```
Device# show flexconnect url-acl

ACL-NAME          ACTION      URL-LIST

SplitTunnelACL    deny        base.com
```

AP Survey Mode

To enable the Cisco Catalyst 9136 Series APs and other upcoming AP models for site survey at customer sites, a new AP command is introduced to help APs to switch to survey mode. When an AP is in survey mode, the AP GUI is enabled and is used for configuring the RF parameters for site survey investigation.

To enable survey mode on an AP, run the **ap-type site-survey** command from the AP CLI.

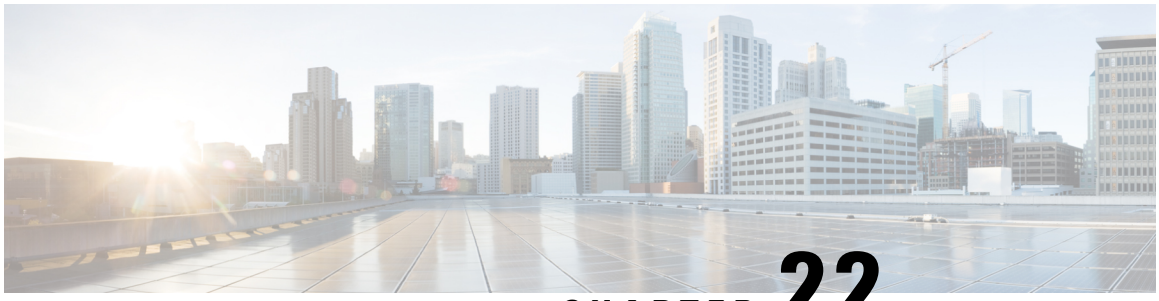
The following features in the AP GUI are hidden, when the AP is in the survey mode:

- WAN
- Firewall
- Network Diagnostics

Note To make the hidden features visible on the AP GUI, you must switch the AP back to the CAPWAP mode, by running the **ap-type capwap** command from the AP CLI. In CAPWAP mode, the AP GUI becomes available only when the **OfficeExtend AP** field is enabled in the flex profile page associated to that AP.

Note To access the AP survey mode from the GUI, you must enter the default login as 'admin' and the default password as 'admin' (both case sensitive).

When the AP is in survey mode, it broadcasts an SSID by default. The default password to connect to this SSID is 'password' (case sensitive).



CHAPTER 22

Security

- Information About Data Datagram Transport Layer Security, on page 387
- Configuring Data DTLS (GUI), on page 388
- Configuring Data DTLS (CLI), on page 388
- Introduction to the 802.1X Authentication, on page 389
- Limitations of the 802.1X Authentication, on page 390
- Topology - Overview, on page 391
- Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI), on page 392
- Configuring 802.1X Authentication Type and LSC AP Authentication Type, on page 392
- Enabling 802.1X on the Switch Port, on page 394
- Verifying 802.1X on the Switch Port, on page 396
- Verifying the Authentication Type, on page 397

Information About Data Datagram Transport Layer Security

Data Datagram Transport Layer Security (DTLS) enables you to encrypt CAPWAP data packets that are sent between an access point and the controller using DTLS, which is a standards-track IETF protocol that can encrypt both control and data packets based on TLS. CAPWAP control packets are management packets that are exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data).

If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

If an access point supports Data DTLS, it enables data DTLS after receiving the new configuration from the controller . The access point performs a DTLS handshake on port 5247 and after successfully establishing the DTLS session. All the data traffic (from the access point to the controller and the controller to the access point) is encrypted.

Note The throughput is affected for some APs that have data encryption enabled.

The controller does not perform a DTLS handshake immediately after processing client-hello with a cookie, if the following incorrect settings are configured:

- ECDHE-ECDSA cipher in “ap dtls-cipher <>” and RSA-based certificate in “wireless management trustpoint”.
- RSA cipher in “ap dtls-cipher <>” and EC-based certificate in “wireless management trustpoint”.

Note This is applicable when you move from CC -> FIPS -> non-FIPS mode.

Note If the AP’s DHCP lease time is less and the DHCP pool is small, access point join failure or failure in establishing the Data Datagram Transport Layer Security (DTLS) session may occur. In such scenarios, associate the AP with a named site-tag and increase the DHCP lease time for at least 8 days.

Configuring Data DTLS (GUI)

Follow the procedure to enable DTLS data encryption for the access points on the controller :

Procedure

Step 1 Click **Configuration** > **Tags and Profile** > **AP Join**.

Step 2 Click **Add** to create a new **AP Join Profile** or click an existing profile to edit it.

Step 3 Click **CAPWAP** > **Advanced**.

Step 4 Check **Enable Data Encryption** check box to enable Datagram Transport Layer Security (DTLS) data encryption.

Step 5 Click **Update & Apply to Device**.

Configuring Data DTLS (CLI)

Follow the procedure given below to enable DTLS data encryption for the access points on the controller :

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:**	Configures an AP profile and enters AP profile configuration mode.

	Command or Action	Purpose
	`Device(config)# ap profile test-ap-profile`	**Note** You can use the default AP profile (default-ap-profile) or create a named AP profile, as shown in the example.

Step 3	**link-encryption**
	Example:
	`Device(config-ap-profile)# link-encryption`
		Enables link encryption based on the profile. Answer yes, when the system prompts you with this message:
		Note If you set stats-timer as as zero (0) under the AP profile, then the AP will not send the link encryption statistics.
		`Enabling link-encryption will reboot the APs with link-encryption.`
		`Are you sure you want to continue? (y/n)[y]:`

Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.
Step 5	**show wireless dtls connections** **Example:** `Device# show wireless dtls connections`	(Optional) Displays the DTLS session established for the AP that has joined this controller.
Step 6	**show ap link-encryption** **Example:** `Device# show ap link-encryption`	(Optional) Displays the link encryption-related statistics (whether link encryption is enabled or disabled) counter received from the AP.

Introduction to the 802.1X Authentication

IEEE 802.1X port-based authentication is configure on a device to prevent unauthorized devices from gaining access to the network. The device can combine the function of a router, switch, and access point, depending on the fixed configuration. Any device connecting to a switch port where 802.1X authentication is enabled must go through relevant EAP authentication model to start exchanging traffic.

Currently, the Cisco Wave 2 and Wi-Fi 6 (802.11AX) APs support 802.1X authentication with switch port for EAP-FAST, EAP-TLS and EAP-PEAP methods. Now, you can enable configurations and provide credentials to the AP from the controller .

Note If the AP is dot1x EAP-FAST, when the AP reboots, it should perform an anonymous PAC provision. For performing PAC provision, the ADH cipher suites should be used to establish an authenticated tunnel. If the ADH cipher suites are not supported by radius servers, AP will fail to authenticate on reload.

EAP-FAST Protocol

In the EAP-FAST protocol developed by Cisco, in order to establish a secured TLS tunnel with RADIUS, the AP requires a strong shared key (PAC), either provided via in-band provisioning (in a secured channel) or via out-band provisioning (manual).

Note The EAP-FAST type configuration requires 802.1x credentials configuration for AP, since AP will use EAP-FAST with MSCHAP Version 2 method.

Note Local EAP is not supported on the Cisco 7925 phones.

Note In Cisco Wave 2 APs, for 802.1x authentication using EAP-FAST after PAC provisioning (caused by the initial connection or after AP reload), ensure that you configure the switch port to trigger re-authentication using one of the following commands: **authentication timer restart** *num* or **authentication timer reauthenticate** *num*.

Starting from Cisco IOS XE Amsterdam 17.1.1, TLS 1.2 is supported in EAP-FAST authentication protocol.

EAP-TLS/EAP-PEAP Protocol

The EAP-TLS protocol or EAP-PEAP protocol provides certificate based mutual EAP authentication.

In EAP-TLS, both the server and the client side certificates are required, where the secured shared key is derived for the particular session to encrypt or decrypt data. Whereas, in EAP-PEAP, only the server side certificate is required, where the client authenticates using password based protocol in a secured channel.

Note The EAP-PEAP type configuration requires Dot1x credentials configuration for AP; and the AP also needs to go through LSC provisioning. AP uses the PEAP protocol with MSCHAP Version 2 method.

Limitations of the 802.1X Authentication

- 802.1X is not supported on dynamic ports or Ethernet Channel ports.
- 802.1X is not supported in a mesh AP scenario.
- There is no recovery from the controller on credential mismatch or the expiry/invalidity of the certificate on AP. The 802.1X authentication has to be disabled on the switch port to connect the AP back to fix the configurations.
- There are no certificate revocation checks implemented on the certificates installed in AP.

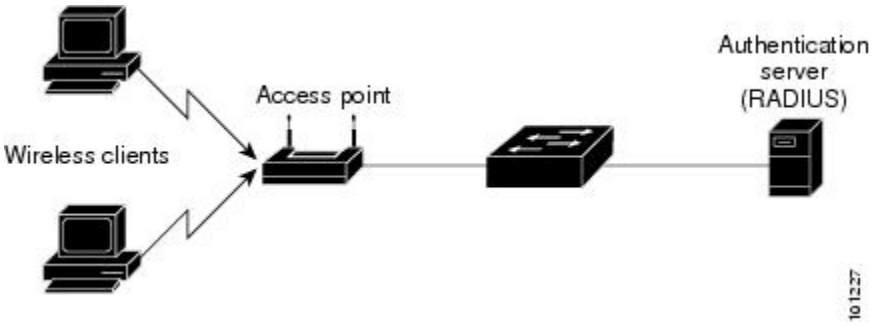
- Only one Locally Significant Certificates (LSC) can be provisioned on the AP and the same certificate must be used for CAPWAP DTLS session establishment with controller and the 802.1X authentication with the switch. If global LSC configuration on the controller is disabled; AP deletes LSC which is already provisioned.
- If clear configurations are applied on the AP, then the AP will lose the 802.1X EAP type configuration and the LSC certificates. AP should again go through staging process if 802.1X is required.
- 802.1X for trunk port APs on multi-host authentication mode is supported. Network Edge Authentication Topology (NEAT) is not supported on COS APs.
- The DHCP requests are sent in incremental periodic value of: "2, 3, 4, 6, 8, 11, 15, 20, 27, 30, 30, 30, 30, 30...". The Cisco Catalyst 9100 Access Points perform an interface reset following a 100-second timeout, which in turn resets the timers on the associated switch port to which they are connected.

Topology - Overview

The 802.1X authentication events are as follows:

1. The AP acts as the 802.1X supplicant and is authenticated by the switch against the RADIUS server which supports EAP-FAST along with EAP-TLS and EAP-PEAP. When dot1x authentication is enabled on a switch port, the device connected to it authenticates itself to receive and forward data other than 802.1X traffic.
2. In order to authenticate with EAP-FAST method, the AP requires the credentials of the RADIUS server. It can be configured at the controller , from where it will be passed on to the AP via configuration update request. For, EAP-TLS or EAP-PEAP the APs use the certificates (device/ID and CA) made significant by the local CA server.

Figure 17: Figure: 1 Topology for 802.1X Authentication



Configuring 802.1X Authentication Type and LSC AP Authentication Type (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** page, click **Add**.

The **Add AP Join Profile** page is displayed.

Step 3 In the **AP** > **General** tab, navigate to the **AP EAP Auth Configuration** section.

Step 4 From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP* to configure the dot1x authentication type.

Step 5 From the **AP Authorization Type** drop-down list, choose the type as either CAPWAP DTLS + or CAPWAP DTLS.

Step 6 Click **Save & Apply to Device**.

Configuring 802.1X Authentication Type and LSC AP Authentication Type

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap profile** *profile-name* **Example:** `Device(config)# ap profile new-profile`	Specify a profile name.
Step 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type. **max-sessions**: Configures the maximum 802.1X sessions initiated per AP.

	Command or Action	Purpose
		username: Configures the 802.1X username for all Aps. **eap-type:** Configures the dot1x authentication type with the switch port. **lsc-ap-auth-state**: Configures the LSC authentication state on the AP.
Step 5	**dot1x eap-type {EAP-FAST | EAP-TLS | EAP-PEAP}** **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type: EAP-FAST, EAP-TLS, or EAP-PEAP.
Step 6	**dot1x lsc-ap-auth-state {CAPWAP-DTLS | Dot1x-port-auth | Both}** **Example:** `Device(config-ap-profile)#dot1x lsc-ap-auth-state Dot1x-port-auth`	Configures the LSC authentication state on the AP. **CAPWAP-DTLS**: Uses LSC only for CAPWAP DTLS. **Dot1x-port-auth**: Uses LSC only for dot1x authentication with port. **Both**: Uses LSC for both CAPWAP-DTLS and Dot1x authentication with port.
Step 7	**end** **Example:** `Device(config-ap-profile)# end`	Exits the AP profile configuration mode and enters privileged EXEC mode.

Configuring the 802.1X Username and Password (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.
Step 2 On the **AP Join** page, click the name of the AP Join profile or click **Add** to create a new one.
Step 3 Click the **Management** tab and then click the **Credentials** tab.
Step 4 Enter the local username and password details.
Step 5 Choose the appropriate local password type.
Step 6 Enter 802.1X username and password details.
Step 7 Choose the appropriate 802.1X password type.
Step 8 Enter the time in seconds after which the session should expire.
Step 9 Enable local credentials and/or 802.1X credentials as required.
Step 10 Click **Update & Apply to Device**.

Configuring the 802.1X Username and Password (CLI)

The following procedure configures the 802.1X password for all the APs:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap profile** *profile-name* **Example:** `Device(config)# ap profile new-profile`	Specify a profile name.
Step 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** **Example:** `Device(config-ap-profile)# dot1x eap-type`	Configures the dot1x authentication type. **max-sessions**: Configures the maximum 802.1X sessions initiated per AP. **username**: Configures the 802.1X username for all Aps. **eap-type:** Configures the dot1x authentication type with the switch port. **lsc-ap-auth-state**: Configures the LSC authentication state on the AP.
Step 5	**dot1x username** <username> **password {0 | 8}** <password> **Example:** `Device(config-ap-profile)#dot1x username username password 0 password`	Configures the dot1x password for all the APs. 0: Specifies an unencrypted password will follow. 8: Specifies an AES encrypted password will follow.

Enabling 802.1X on the Switch Port

The following procedure enables 802.1X on the switch port:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication dot1x {default | listname} method1[method2...]** **Example:** `Device(config)# aaa authentication dot1x default group radius`	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server.
Step 5	**aaa authorization network group** **Example:** `aaa authorization network group`	Enables AAA authorization for network services on 802.1X.
Step 6	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 7	**interface type slot/port** **Example:** `Device(config)# interface fastethernet2/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 8	**authentication port-control {auto | force-authorized | force-unauthorized}** **Example:** `Device(config-if)# authentication port-control auto`	Enables 802.1X port-based authentication on the interface. **auto**—Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The Device requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant

	Command or Action	Purpose
		attempting to access the network is uniquely identified by the Device by using the supplicant MAC address. **force-authorized**-—Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting. **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The Device cannot provide authentication services to the supplicant through the port.
Step 9	**dot1x pae [supplicant | authenticator | both]** **Example:** `Device(config-if)# dot1x pae authenticator`	Enables 802.1X authentication on the port with default parameters.
Step 10	**end** **Example:** `Device(config-if)# end`	Enters privileged EXEC mode.

Verifying 802.1X on the Switch Port

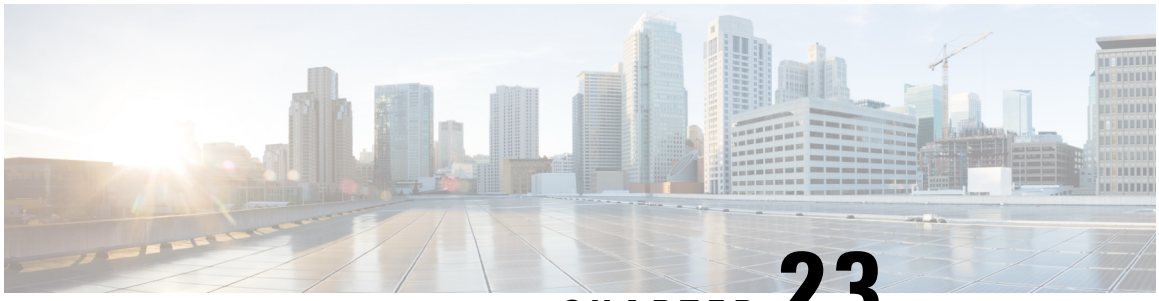
The following show command displays the authentication state of 802.1X on the switch port:

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version      2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Device#
```

Verifying the Authentication Type

The following show command displays the authentication state of an AP profile:

```
Device#show ap profile <profile-name> detailed ?
  chassis  Chassis
  |        Output modifiers
  <cr>

Device#show ap profile <profile-name> detailed

  AP Profile Name        : default-ap-profile
  Description            : default ap profile
  …
  Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
  LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth
```



CHAPTER 23

AP Joining

- Failover Priority for Access Points, on page 399
- Setting AP Priority (GUI), on page 400
- Setting AP Priority, on page 400
- Overview of Access Point Plug-n-Play, on page 400
- Provisioning AP from PnP Server, on page 401
- Verifying AP Tag Configuration, on page 401
- Feature History for AP Fallback to Controllers Using AP Priming Profile, on page 402
- Information About AP Fallback to Controllers Using AP Priming Profile, on page 402
- Restrictions for AP Fallback to Controllers Using AP Priming Profile, on page 402
- Configure AP Priming Profile, on page 403
- Configure AP Priming Using Filters, on page 404
- Configure Per-AP Priming, on page 405
- Verify the Configuration, on page 405

Failover Priority for Access Points

Each controller has a defined number of communication ports for access points. When multiple controllers with unused access point ports are deployed on the same network and one controller fails, the dropped access points automatically poll for unused controller ports and associate with them.

The following are some guidelines for configuring failover priority for access points:

- You can configure your wireless network so that the backup controller recognizes a join request from a higher-priority access point, and if necessary, disassociates a lower-priority access point as a means to provide an available port.
- Failover priority is not in effect during the regular operation of your wireless network. It takes effect only if there are more associations requests to controller than the available AP capacity on the controller.
- AP priority is checked while connecting to the controller when the controller is in full scale or the primary controller fails, the APs fallback to the secondary controller.
- You can enable failover priority on your network and assign priorities to the individual access points.
- By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

Setting AP Priority (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the Access Point.

Step 3 In the **Edit AP** dialog box, go to **High Availability** tab.

Step 4 Choose the priority from the **AP failover priority** drop-down list.

Step 5 Click **Update and Apply to Device**.

Setting AP Priority

Note Priority of access points ranges from 1 to 4, with 4 being the highest.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **priority** *priority* **Example:** `Device# ap name AP44d3.ca52.48b5 priority 1`	Specifies the priority of an access point.
Step 2	**show ap config general** **Example:** `Device# show ap config general`	Displays common information for all access points.
Step 3	**show ap name** *ap-name* **config general** **Example:** `Device# show ap name AP44d3.ca52.48b5 config general`	Displays the configuration of a particular access point.

Overview of Access Point Plug-n-Play

The Plug and Play (PnP) server provides staging parameters to an access point (AP) before it joins a controller. Using this staging configuration, the AP receives the runtime configuration when it joins the controller.

The AP PnP feature enables the PnP server to provide all tag-related information, as part of the preconfigured information to the AP and in turn, to the controller.

You can upload configuration in PNP server in either *TXT* or *JSON* format and also add the AP details. The AP details are then mapped with the details in the *TXT* or *JSON* configuration file. While provisioning AP from PnP server, the AP acquires this configuration details. Based on the configuration details, the AP then joins the corresponding controller with the tag details.

Provisioning AP from PnP Server

You can provision AP from PnP Server in either ways:

- Configure DHCP server or switch with *Option 43*. For example, you can refer to the following code sample:

```
ip dhcp pool vlan10
 network 9.10.10.0 255.255.255.0
 default-router 9.10.10.1
  option 43 ascii 5A1D;B2;K4;|9.10.60.5;J80
```

- Configure DHCP server with DNS. For example, you can refer to the following code sample:

```
ip dhcp pool vlan10
 network 9.10.10.0 255.255.255.0
 default-router 9.10.10.1
 dns-server 9.8.65.5
 domain-name dns.com
```

Verifying AP Tag Configuration

The following example shows how to verify the AP tag configuration:

```
Device# show ap tag summary
Number of APs: 5


AP Name                 AP Mac           Site Tag Name           Policy Tag Name
RF Tag Name             Misconfigured    Tag Source

-------------------------------------------------------------------------------

APd42c.4482.6102        d42c.4482.6102   default-site-tag        default-policy-tag
default-rf-tag          No               Default

AP00c1.64d8.6af0        00c1.64d8.6af0   named-site-tag          named-policy-tag
named-rf-tag            No               AP
```

Note The details in the second row reflect the tag source coming from a PNP server.

Feature History for AP Fallback to Controllers Using AP Priming Profile

This table provides release and related information for the feature explained in this module.

Table 27: Feature History for AP Fallback to Controllers Using AP Priming Profile

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.2	AP Fallback to Controllers Using AP Priming Profile	This feature helps to configure primary, secondary, and tertiary controllers for a group of APs matching regular expression or for an individual AP using priming profiles.

Information About AP Fallback to Controllers Using AP Priming Profile

In large networks, accessing every AP console and configuring AP priming for primary, secondary, and tertiary controllers are not easy tasks. The AP Fallback to Controllers Using AP Priming Profile feature allows you to simplify the task of priming APs by using profiles defined in the controller.

Using the AP priming profile under the AP filter profile, you can configure primary, secondary, and tertiary controllers for a group of APs matching regular expressions, or for an individual AP using AP Ethernet MAC. When the AP joins the controller, the AP priming configuration gets pushed to the AP depending on whether priming override is enabled or not.

Note When the controller sends a priming profile to the AP, the AP disconnects from the current controller and joins the controller in the priming profile. A CAPWAP restart or device reboot is not required.

Restrictions for AP Fallback to Controllers Using AP Priming Profile

- Rolling AP upgrade will not work if priming override is enabled.
- The maximum number of priming profiles permitted is 128. The length of each profile can be up to 32 ASCII characters.

Configure AP Priming Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile ap priming** *profile-name* **Example:** `Device(config)# wireless profile ap priming Prime-FX`	Configures the profile to prime APs.
Step 3	**primary** *controller-name ip-address* **Example:** `Device(config-priming)# primary aaaa 209.165.201.2`	Configures name and IP address of the primary controller for AP fallback.
Step 4	**secondary** *controller-name ip-address* **Example:** `Device(config-priming)# secondary bbbb 209.165.201.3`	Configures name and IP address of the secondary controller for AP fallback.
Step 5	**tertiary** *controller-name ip-address* **Example:** `Device(config-priming)# tertiary bbbb 209.165.201.4`	Configures name and IP address of the tertiary controller for AP fallback.
Step 6	**priming-override** **Example:** `Device(config-priming)# priming-override`	Sends the priming details to the AP. Priming override is disabled by default. When disabled, information stored in the AP priming profile is not sent to the APs. . **Note** N+1 upgrade may not work as expected when priming override is enabled. Before using N+1 upgrade, ensure that priming override is disabled using the **no priming-override** command.

Configure AP Priming Using Filters

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap filter name** *filter-name* **type priming** **Example:** `Device(config)# ap filter name test-filter type priming`	Configures the AP filter and sets the type as priming. Ensure that you set type as priming because the default filter type is tag. **Note** The existing filter type cannot be modified unless the filter is deleted and created with a different type. Use the **no ap filter name** command to delete a filter.
Step 3	**ap name-regex** *reg-ex* **Example:** `Device(config-ap-pr-filter)# ap name-regex BGL18`	Configures the AP name regular expression match.
Step 4	**profile** *profile-name* **Example:** `Device(config-ap-pr-filter)# profile Prime-FX`	Maps the priming profile to the filter.
Step 5	**exit** **Example:** `Device(config-ap-pr-filter)# exit`	Returns to global configuration.
Step 6	**ap filter priority** *priority* **filter-name** *filter-name* **Example:** `Device(config)# ap filter priority 12 filter-name test-filter`	Configures priority for a named AP filter. You can configure multiple AP priming profiles with unique priority levels. This allows you to set different priority levels for each AP priming profile.

Configure Per-AP Priming

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap 00:00:5e:00:53:af`	Enters AP profile configuration mode.
Step 3	**priming** *profile-name* **Example:** `Device(config-ap-tag)# priming Prime-FX`	Maps a priming profile to an AP.

Verify the Configuration

To view the list of all the priming filters, use the following command:

```
Device# show ap filters all type priming

Filter Name                        regex                              Priming profile
-------------------------------------------------------------------------------------------
FLR1                                *AP-FLOOR-1*                      AP-PRIMING-1

FLR2                                *AP-FLOOR-2*                      AP-PRIMING-2
```

To view the list of all the active priming filters, use the following command:

```
Device# show ap filters active type priming

Priority   Filter Name              regex                            Priming profile

-------------------------------------------------------------------------------------------

 0          FLR2                    *AP-FLOOR-2*                     AP-PRIMING-2

 1          FLR1                    *AP-FLOOR-1*                     AP-PRIMING-1
```

To view the summary of the priming profiles, use the following command:

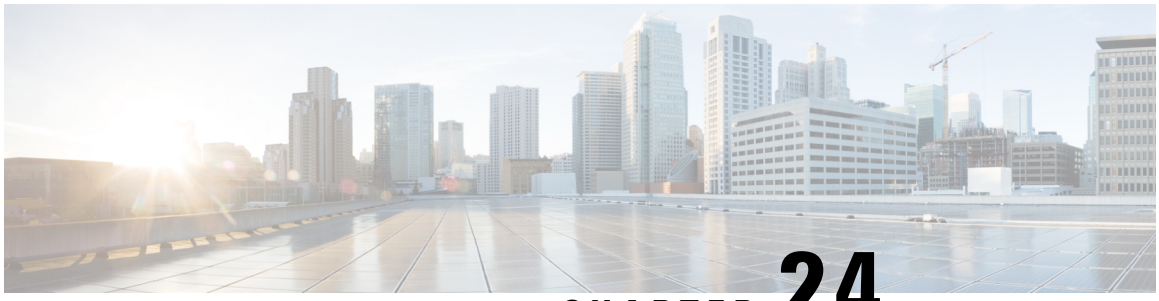
```
Device# show wireless profile ap priming summary

Number of AP Priming Profiles: 2
Priming profile
-------------------
AP-PRIMING-1
AP-PRIMING-2
```

To view the details of the priming profiles, use the following command:

```
Device# show wireless profile ap priming all

Profile Name  Primary Controller Name  Primary Controller IP  Secondary Controller Name
Secondary Controller IP  Tertiary Controller Name  Tertiary Controller IP  Override
------------------------------------------------------------------------------------------------------------------------------------
AP-PRIMING-1  BGL18-wlc               209.165.201.1          BGL17-wlc
209.165.201.2                                    0.0.0.0               Disabled
AP-PRIMING-2  BGL18-wlc               209.165.201.2          BGL17-wlc
209.165.201.2            BGL12-wlc                209.165.201.3          Disabled
```

To view the priming information for each AP, use the following command:

```
Device# show ap ap1 config general | sec Priming

Priming Profile                  : AP-PRIMING-1
Priming Override                 : Disabled
Priming Source                   : MAC/FILTER/NONE
Filter Name                      : FLR1
```



CHAPTER 24

AP Management

- AP Crash File Upload, on page 408
- Configuring AP Crash File Upload (CLI), on page 409
- Information About LED States for Access Points, on page 409
- Configuring LED State in Access Points (GUI), on page 410
- Configuring LED State for Access Points in the Global Configuration Mode (CLI), on page 410
- Configuring LED State in the AP Profile, on page 411
- Verifying LED State for Access Points, on page 411
- Access Point Support Bundle, on page 412
- Exporting an AP Support Bundle (GUI), on page 412
- Exporting an AP Support Bundle (CLI), on page 413
- Monitoring the Status of Support Bundle Export, on page 413
- Information About Access Point Memory Information, on page 413
- Verifying Access Point Memory Information, on page 414
- Information About Access Point Tag Persistency, on page 414
- Configuring AP Tag Persistency (GUI), on page 414
- Configuring AP Tag Persistency (CLI), on page 415
- Verifying AP Tag Persistency, on page 416
- Feature History for AP Power Save, on page 417
- Information About AP Power Save, on page 417
- Wakeup Threshold for Access Point Power Save Mode, on page 424
- AP Power Save Scenarios, on page 424
- Configuring Power Policy Profile (GUI), on page 426
- Configuring a Power Policy Profile (CLI), on page 426
- Configuring a Calendar Profile (GUI), on page 429
- Configuring a Calendar Profile (CLI), on page 430
- Configuring a Power Policy in an AP Join Profile (GUI), on page 431
- Mapping a Power Profile Under an AP Profile (CLI), on page 431
- Configuring Client Wakeup Threshold (CLI), on page 432
- Configuring PoE-Out Interface in Power Profile (GUI), on page 433
- Configuring PoE-Out Interface in Power Profile (CLI), on page 433
- Configuration Example of Power Profile, on page 434
- Verifying Access Point Power Policy (GUI), on page 434
- Verifying the Access Point Power Profile, on page 435

• Verifying Radio Spatial Streams, on page 436
• Verifying Client Threshold, on page 437
• Verifying PoE-Out Details, on page 437
• Information About Access Point Real-Time Statistics, on page 437
• Feature History for Real Time Access Point Statistics, on page 438
• Restrictions for AP Radio Monitoring Statistics , on page 438
• Configuring Access Point Real Time Statistics (GUI), on page 438
• Configuring Real-Time Access Point Statistics (CLI), on page 439
• Configuring AP Radio Monitoring Statistics, on page 441
• Monitoring Access Point Real-Time Statistics (GUI), on page 442
• Verifying Access Point Real-Time Statistics, on page 443

AP Crash File Upload

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the device. If the unit rebooted because of a crash, the device pulls up the crash file using the existing CAPWAP messages and stores it in the device flash memory. The crash information copy is removed from the access point's flash memory when the device pulls it from the access point:

Note The system does not generate reports in case of a reload.

During a process crash, the following are collected locally from the device:

- Full process core
- Trace logs
- Cisco IOS syslogs (not guaranteed in case of nonactive crashes)
- System process information
- Bootup logs
- Reload logs
- Certain types of proc information

All this information is stored in separate files, which are then archived and compressed into one bundle. This makes it convenient to get a crash snapshot in one place, and can be then moved off the box for analysis. This report is generated before the device goes down to ROMMON/bootloader.

Note Except for the full core and tracelogs, everything else is a text file.

Configuring AP Crash File Upload (CLI)

Procedure

Step 1 **enable**

Enters privileged EXEC mode.

Step 2 **ap name** *ap-name* **crash-file get-crash-data**

Collects AP crash information. The crash file is uploaded automatically after the AP reloads to ready state. Therefore, this command does not have to be manually executed.

Step 3 **ap name** *ap-name* **crash-file get-radio-core-dump slot** {**0** | **1**}

Collects the AP core dump file for slot 0 or slot 1.

Step 4 **ap name** *ap-name* **core-dump** *tftp-ip crash-file* **uncompress**

Uploads the AP crash coredump file to the given TFTP location.

Step 5 **show ap crash-file**

Displays the AP crash file, as well as the radio crash file.

Step 6 **dir bootflash**

Displays the crash file in bootflash with .crash extension.

Information About LED States for Access Points

In a wireless LAN network where there are a large number of access points, it is difficult to locate a specific access point associated with the controller. You can configure the controller to set the LED state of an access point so that it blinks and the access point can be located. This configuration can be done in the wireless network on a global as well as per-AP level.

The LED state configuration at the global level takes precedence over the AP level.

Note For APs that have Ethernet LEDs in addition to the main system LED, the Ethernet LEDs are enabled or disabled (switched ON or OFF) as per the system LED. For example, if the system LED is ON, the Ethernet LED will also be ON.

Configuring LED State in Access Points (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click an AP from the AP list.
The **Edit AP** window is displayed.

Step 3 In the **General** tab, under the General section, go to **LED Settings**.

a) Click the box adjacent to the **LED State** field to enable or disable the LED state.

b) From the **LED Brightness Level** drop-down list, choose a value from 1 to 8.

Step 4 Under the **Flash Settings** section, perform the following steps:

a) Click the box adjacent to the **Flash State** field to enable or disable the flash state.
When the flash state is enabled, the current status of the flash and the flash duration fields are displayed.

b) From the **Flash Duration** drop-down list, choose either **Always ON** or **Timed**.
If you choose the **Timed** option, the **Time Duration** field is displayed.

c) In the **Time Duration** field, specify the flash duration time, in seconds. The default value is one second. The valid range is between 1 second and 3600 seconds.

Step 5 Click **Update & Apply to Device**.

Configuring LED State for Access Points in the Global Configuration Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**ap name** *Cisco-AP-name* **led** **Example:** `Device# ap name Cisco-AP-name led`	Enables the LED state for Cisco APs, globally.
Step 3	**ap name** *Cisco-AP-name* **led flash** {**start duration** *duration* | **stop**} **Example:** `Device# ap name Cisco-AP-name led flash start duration 20`	Configures the starting and the stopping of the AP LED flash. The valid start duration range is between 0 and 3600 seconds.

	Command or Action	Purpose
	`Device# ap name Cisco-AP-name led flash stop`	
Step 4	**ap name** *Cisco-AP-name* **led-brightness-level** *1-8* **Example:** `Device# ap name Cisco-AP-name led-brightness-level 4`	Configures the LED brightness level. Value of the brightness is from 1 to 8.

Configuring LED State in the AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *default-ap-profile* **Example:** `Device(config)#ap profile default-ap-profile`	Enters the AP profile configuration mode.
Step 3	**led** **Example:** `Device(config-ap-profile)# led`	Enables the LED-state for all Cisco APs.

Verifying LED State for Access Points

To verify the LED state of the access points, use the following command:

show ap name AXXX-APXXXX.bdXX.f2XX config general

```
Device# show ap name AXXX-APXXXX.bdXX.f2XX config general
Cisco AP Name : AXXX-APXXXX.bdXX.f2XX
================================================
Cisco AP Identifier : 0cXX.bdXX.65XX
Country Code : Multiple Countries : FR,IN,US
Regulatory Domain Allowed by Country : 802.11bg:-AE 802.11a:-ABDEN
AP Country Code : US - United States
AP Regulatory Domain
802.11bg : -A
802.11a : -B
.
.
.
CAPWAP Preferred mode : IPv4
```

```
CAPWAP UDP-Lite : Not Configured
AP Submode : WIPS
Office Extend Mode : Disabled
Dhcp Server : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : information
Logging Syslog facility : kern
Software Version : 17.X.0.XXX
Boot Version : 1.1.X.X
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
MDNS Group Id : 0
.
.
.
```

Access Point Support Bundle

An access point (AP) support bundle contains core files, crash files, **show run-configuration**, configuration commands, msglogs, and traplogs.

This topic describes how you can retrieve the support bundle information of an AP and export it to the controller or to an external server. (Until Cisco IOS XE, Release 17.2.1, you had to log in to the AP console to retrieve the AP support-bundle information.)

The Access Point Support Bundle feature is supported only on Cisco Wave2 APs and Cisco Catalyst APs.

Exporting an AP Support Bundle (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the corresponding AP name.
The **Edit AP** window is displayed.

Step 3 Click the **Support Bundle** tab.

Step 4 From the **Destination** drop-down list, choose one of the following:

- **This Device**: If you choose this, enter the values for the **Server IP**, **Destination File Path**, **Username**, and **Password** fields.

  Note When you choose **This Device**, a bundle is sent through Secure Copy (SCP) to the controller (if you have configured the **ip scp server enable** command globally on the controller). You can easily retrieve the bundle later from your browser, using the controller file manager.

- **External Server**: If you choose this, from the **Transfer Mode** drop-down list, choose either **scp** or **tftp**.

  If you choose the **scp** transfer mode, enter the values for the **Server IP**, **Destination File Path**, **Username**, and **Password** fields.

  If you choose the **tftp** transfer mode, enter the values for the **Server IP**, and **Destination File Path** fields.

Note Information about the **Last Export Status**, such as **State**, **Transfer Mode**, **Server IP**, **File Path**, and **Time of Export**, is displayed on the right-hand side of the window.

Step 5 Click **Start Transfer**.

Exporting an AP Support Bundle (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**ap name** *Cisco-AP-name* **export support-bundle mode** { **scp** | **tftp** } **target ip-address** {*A.B.C.D* | *X:X:X:X::X*} **path** *file-path* **Example:** `Device> ap name Cisco-AP-name export support-bundle mode scp target ip-address 10.1.1.1 path file-path`	Exports the AP support bundle through the SCP or TFTP transfer modes. If you select the **scp**, you will be prompted to provide your username and password. For **tftp**, username and password is not required.

Monitoring the Status of Support Bundle Export

To monitor the status of a support bundle export, run the following command:

```
Device# show ap support-bundle summary
AP Name    Server-IP   Status        Last Successful Time      Path File-name
-------------------------------------------------------------------------------
AP_28XXX   81.1.1.10   Copy Success  04/24/2020 07:27:38 UTC
AP_28XXX_support.17.4.0.2.2020.07XXXX.tgz
```

Information About Access Point Memory Information

With the introduction of the Access Point Memory Information feature, you can view the access point (AP) memory type, the CPU type, and the memory size per AP, after single sign-on authentication. APs share the memory information with the controller during the join phase.

To view the memory information of a specific AP, use the **show ap name** *AP-NAME***config general** command.

Verifying Access Point Memory Information

To verify the memory information of a specified AP, including the CPU type, memory type and memory size, use the following command:

```
Device# show ap name AP-NAME  config general
Cisco AP Name   : AP-NAME
================================================
Cisco AP Identifier                             : 00XX.f1XX.e0XX
Country Code                                    : Multiple Countries : FR,IN,US
Regulatory Domain Allowed by Country            : 802.11bg:-AE   802.11a:-ABDEN
AP Country Code                                 : US  - United States
AP Regulatory Domain
  802.11bg                                      : -A
  802.11a                                       : -B
.
.
.
CPU Type                                        : ARMv7 Processor rev 1 (v7l)
Memory Type                                     : DDR4
Memory Size                                     : 1028096 KB
.
.
.
```

Information About Access Point Tag Persistency

From Cisco IOS XE Bengaluru 17.6.1 onwards, AP tag persistency is enabled globally on the controller. When APs join a controller with tag persistency enabled, the mapped tags are saved on the APs without having to write the tag configurations on each AP, individually.

Configuring AP Tag Persistency (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 Click the **AP** tab.

Step 3 In the **Tag Source** tab, check the **Enable AP Tag Persistency** check box to configure AP Tag persistency globally.

When APs join a controller with the tag persistency enabled, the mapped tags are saved on the AP without having to write the tag configurations on each AP individually.

Step 4 Click **Apply to Device**.

What to do next

Save tags on an AP.

Saving Tags on an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click an AP from the list.
The **Edit AP** page is displayed.

Step 3 Click the **General** tab.

Step 4 In the **Tags** section, specify the appropriate policy, site, and RF tags that you created in the **Configuration** > **Tags & Profiles** > **Tags** page.

Step 5 From the **Policy** drop-down list, select a value.

Step 6 From the **Site** drop-down list, select a value.

Step 7 From the **RF** drop-down list, select a value.

Step 8 Check the **Write Tag Config to AP** check box to push the tags to the AP so that the AP can save and remember this information even when the AP is moved from one controller to another.

Step 9 Click **Update & Apply to Device**.

Deleting Saved Tags on the Access Point

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click an AP from the list of APs.
The **Edit AP** window is displayed.

Step 3 In the **Edit AP** window, choose the **Advanced** tab.

Step 4 In the **Set to Factory Default** section, check the **Clear Resolved Tag Config** check box to clear the saved tags on an AP.

Step 5 Click **Update & Apply to Device**.

Configuring AP Tag Persistency (CLI)

Before you begin

For an AP to preserve its policy tag, site tag, and RF tag configured from the primary controller, these tags must also exist on the other controllers that the AP connect to. If all the three tags do not exist, the AP applies the default policy tag, site tag, and RF tag. Similarly, the tag policy is applicable even if one or two tags exist. AP tag persistency helps in priming an AP in N+1 redundancy scenarios. For more information about configuring tags, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_config_model.html.

Note After being enabled, AP tag persistency is performed during AP join. Therefore, if there are any APs that are already joined to the controller, those APs must rejoin the controller.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap tag persistency enable** **Example:** `Device(config)# ap tag persistency enable`	Configures AP tag persistency.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying AP Tag Persistency

To verify AP tag persistency in the primary controller, use the following command:

```
Device# show ap tag summary
Number of APs: 1

AP Name         AP Mac           Site Tag Name         Policy Tag Name        RF Tag Name
          Misconfigured    Tag Source
-------------------------------------------------------------------------------------------
Cisco01_AP      xxxx.xxxx.xxxx   default-site-tag      OpenRoaming           default-rf-tag
         No               Static
```

Note If the Tag Source displays **Static** or **Filter**, it means that the AP tag mappings were configured on the primary controller. If the source displays **Default**, it means that the AP received the default tags when joining the controller.

To verify the AP tag persistency in the secondary controller, use the following command:

```
Device# show ap tag summary
Number of APs: 1

AP Name       AP Mac           Site Tag Name        Policy Tag Name     RF Tag Name
Misconfigured   Tag Source
-------------------------------------------------------------------------------------------
Cisco01_AP   xxxx.xxxx.xxxx    default-site-tag     OpenRoaming         default-rf-tag
 No              AP
```

Note If the Tag Source displays **AP**, it means that the policy tag, site tag, and RF tag match what was configured on the primary controller, indicating that the AP tags have persisted across controllers.

Feature History for AP Power Save

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 28: Feature History for AP Power Save

Release	Feature Information
Cisco IOS XE Cupertino 17.8.1	This feature allows a network administrator to force APs to operate in low-power mode to reduce power consumption.
Cisco IOS XE Cupertino 17.9.1	Feature support for the following APs: • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 Series Access Points
Cisco IOS XE Dublin 17.10.1	The following features are supported: • Radio spatial streams • Flexible PoE profiles
Cisco IOS XE 17.13.1	AP Power Distribution support in Cisco Catalyst 9124 Series APs.

Information About AP Power Save

The power-save mode in APs allows a network administrator to force APs to operate in low-power mode to reduce power consumption.

The AP Power Save feature is supported in the following APs:

- Cisco Catalyst 9115 Series Access Points
- Cisco Catalyst 9120 Series Access Points
- Cisco Catalyst 9124 Series Access Points
- Cisco Catalyst 9130 Series Access Points
- Cisco Catalyst 9136 Series Access Points
- Cisco Catalyst 9164 Series Access Points
- Cisco Catalyst 9166 Series Access Points

- Cisco Catalyst 9162 Series Access Points

Access Point Power Policy

The access point power policy allows you to define the power budget utilization available for an AP, wherein, you can define a set of policies for different interfaces on an AP. You can manage interfaces such as Wi-Fi radios, USB, and so on, as required.

Cisco Catalyst 9124 AXI/D APs support up to two radio interfaces (single 5 GHz), and Cisco Catalyst 9124 AXE APs support up to three (dual 5 GHz) radio interfaces. When Cisco Catalyst 9124 Series APs operate under 802.3at/PoE+/30W insufficient power condition, the new operating modes support both dual or Tri-Radio mode.

Use Case for AP Power Policy

The following is the use case of an AP power policy:

- You can define a power policy for the available power inputs, such as, 802.3af, 802.3at, 802.3bt (for multiple levels), DC power, and so on. With tri-radio and quad-radio APs, the power requirement has gone beyond the capability of the 802.3at Power over Ethernet (PoE) mode. Therefore, with the AP power policy, for example, we statically predefine an AP operation when provided with non-802.3bt power (such, as TX power, radio chains, USB port, SFP, and so on).

Power-Save Mode

The power-save mode enables an AP to switch to a low-power mode when no clients are associated with the AP. For example, when this mode is enabled in workspaces, the AP falls asleep during after hours, thereby saving power consumption of the AP throughout the night.

From Cisco IOS-XE Cupertino 17.10.1 onwards, you can shut down AP radios or lower the radio spatial streams, to reduce usage of power. You can enforce radio speed by configuring the number of spatial streams on the radios. The combinations for radio spatial stream policies are: 1X1, 2X2, 3X3 (only for Cisco Catalyst 9130 Series Access Points), 4X4, and 8X8.

The following are the advantages of the power-save mode:

- Increases the energy saving per AP: In the power save mode you can reduce AP functions during off-peak hours and save an additional 20% in energy costs compared to the regular idle mode.
- Enables environmentally conscious purchases: Large enterprises and companies track environmental performance as one of their key indices. They have a centralized energy team to monitor their energy efficiency, which magnifies the importance of the power-save feature.

PoE Profiles

- Fixed PoE Profile: The APs negotiate the power that is required, from the switches they are connected to. The power required varies from one AP model to another AP model. If an AP is not granted the power it requested, it operates under the power budget. In such conditions, some of the interfaces operate under *degraded conditions*.

  For example, some radios may operate at 2SS instead of at 4SS, which they are capable of. The operating conditions for each of the AP interfaces differs from one power level to another. These are referred to

as fixed PoE profiles. Fixed PoE profiles are applied when the AP is operating in normal mode, that is, nonpower-save mode. When the AP operates in power-save mode, the configured PoE power policies are applied.

- PoE Power Policy: With power policies or profiles, you can configure interfaces that you want to set at certain speeds. With this policy, you can configure a profile of your choice that will be pushed to the AP based on your calendar or timing. For example, on a group of APs in the second floor, push a profile where you want to turn off all APs, except 2.4-GHz radio, from 7 p.m. to 7 a.m.
- Flexible PoE Profile: With flexible PoE profiles, you can configure different interfaces and set specific parameter values and states for each interface, instead of following fixed PoE profile rules. If an AP does not get the power it requires, it operates under the power budget by using the flexible PoE profile.

In Cisco IOS XE 17.13.1, PoE-out is a new interface introduced in Cisco Catalyst 9124 Series APs, in addition to the USB, Ethernet, and LAN interfaces. The PoE-out for Cisco Catalyst 9124 Series AP RLAN works only if you have enabled the RLAN port.

The operational parameter values for each interface of the AP may be adjusted based on the AP's hardware specifications as the following Table 2 to 7.

Table 29: AP Power Draw Specifications: Cisco Catalyst 9115, 9120, 9130 Series APs

Access Points	PoE-In-Mode/DC Mode	Consumption @ Power Device	Consumption @ Power Source Equipment	Feature Mode						
		AP	Worst-Case Cable	Radio 1	Radio 2	Radio 3	Ethernet	USB	Module	PoE Out
Cisco Catalyst 9115AXI Access Points	.3af	13.0	15.4	2X2	2X2	—	1G	N	—	—
	.3at	16.0	18.9	4X4	4X4	—	2.5G	N	—	—
	.3at	20.4	24.1	4X4	4X4	—	2.5G	Y(3.75W)	—	—
Cisco Catalyst 9115AXE Access Points	.3af	13.0	15.4	2X2	2X2	—	1G	N	—	—
	.3at	17.0	20.1	4X4	4X4	—	2.5G	N	—	—
	.3at	21.4	25.3	4X4	4X4	—	2.5G	Y(3.75W)	—	—
Cisco Catalyst 9120AXIE Access Points	.3af	13.8	15.4	1X1	1X1	Enabled	1G	N	—	—
	.3at	20.5	23.2	4X4	4X4	Enabled	2.5G	N	—	—
	.3at	25.5	30.0	4X4	4X4	Enabled	2.5G	Y(4.5W)	—	—

Access Points	PoE-In-Mode/DC Mode	Consumption @ Power Device	Consumption @ Power Source Equipment	Feature Mode						
		AP	Worst-Case Cable	Radio 1	Radio 2	Radio 3	Ethernet	USB	Module	PoE-Out
Cisco Catalyst 9130AXIE Access Points	.3af	13.8	15.4	1X1	1X1	Enabled	1G	N	—	—
	.3at	25.5	30.0	8X8	4X4	Enabled	5G	N	—	—
	.3at	25.5	30.0	Primary 4X4 Secondary Off	4X4	Enabled	5G	Y(4.5W)	—	—
	.3at	25.5	30.0	Primary 4X4 Secondary 4X4	Disabled	Enabled	5G	Y(4.5W)	—	—
	.3bt	30.5	33.3	8X8	4X4	Enabled	5G	Y(4.5W)	—	—

Table 30: AP Power Draw Specifications: Cisco Catalyst 9136 Series APs

Access Points	PoE Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode								
		at AP	Worst-Case Cable	5G Radio	2G Radio	6G Radio	AUX Radio	Mgig0	Mgig1	USB	Module	PoE-Out
Cisco Catalyst 9136 Series Access Points	.3af - Fixed	13.9	15.4	Disabled	Disabled	Disabled	Enabled	1G	Disabled	Disabled	—	—
	.3at - Fixed	24.0	27.90	Primary - 4X4 Secondary - Disabled	2X2	2X2	Enabled	2.5G	2.5G (hitless failover standby)	Disabled	—	—
	.3bt - Fixed	43.4	54.81	8X8 or Dual 4X4	4X4	4X4	Enabled	5G	5G	Y(9W)	—	—
	.3bt - PoE Policy 1	37.3	41.63	8X8 or Dual 4X4	4X4	4X4	Enabled	5G	5G	Disabled	—	—

Table 31: AP Power Draw Specifications: Cisco Catalyst 9166 Series APs

Access Points	Power Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode								
		at AP	Worst-Case Cable	5G Radio	2G Radio	6G Radio	AUX Radio	Mgig0	Mgig1	USB	Module	PoE Out
Cisco Catalyst 9166 Series Access Points	.3af - Fixed	13.9	15.4	Disabled	Disabled	Disabled	Enabled	1G	—	Disabled	—	—
	.3at - Fixed Policy	25.5	30.0	4X4	4X4	4X4	Enabled	5G	—	Disabled	—	—
	.3bt - Fixed	30.5	32.8	4X4	4X4	4X4	Enabled	5G	—	Y (4.5 W)	—	—
	DC Jack - Fixed	30.5	—	4X4	4X4	4X4	Enabled	5G	—	Y (4.5 W)	—	—

Table 32: AP Power Draw Specifications: Cisco Catalyst 9164 Series APs

Access Points	Power Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode								
		at AP	Worst-Case Cable	5G Radio	2G Radio	6G Radio	AUX Radio	Mgig0	Mgig1	USB	Module	PoE Out
Cisco Catalyst 9164 Series Access Points	.3af - Fixed	13.9	15.4	Disabled	Disabled	Disabled	Enabled	1G	—	Disabled	—	—
	.3at - Fixed	25.5	30.0	4X4	2X2	4X4	Enabled	2.5G	—	Disabled	—	—
	.3bt - Fixed	30.1	32.8	4X4	2X2	4X4	Enabled	2.5G	—	Y (4.5 W)	—	—
	DC Jack - Fixed	30.1	—	4X4	2X2	4X4	Enabled	2.5G	—	Y (4.5 W)	—	—

Table 33: AP Power Draw Specifications: Cisco Catalyst 9162 Series APs

Access Points	PoE Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode								
		at AP	Worst-Case Cable	5G Radio	2G Radio	6G Radio	AUX Radio	Mgig0	Mgig1	USB	Module	PoE Out
Cisco Catalyst 9162 Series Access Points	.3af	13.3	14.32	1X1	Disabled	1X1	Enabled	1G	—	Disabled	—	—
	.3at	20.1	22.67	2X2	2X2	2X2	Enabled	2.5G	—	Disabled	—	—
	.3at	25.5	30	2X2	2X2	2X2	Enabled	2.5G	—	Y (4.5W)	—	—

Table 34: AP Power Draw Specifications: Cisco Catalyst 9124 Series APs

Access Points	PoE Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode										
		at AP	Worst-Case Cable	Radio 0	R0 dBm Per Path	Radio 1	R1 dBm Per Path	Radio 2	R02 dBm Per Path	AUX Radio	Ethernet Mgig	SFP Module	GbE PHY	PoE Out
				2.4 GHz Radio		5 GHz Primary Radio		5 GHz Secondary Radio		Olwave				
Cisco Catalyst 9124 AXI Cisco Catalyst 9124 AXD Cisco Catalyst 9124 AXE Dual Radio Mode	.3af	13.8	15.4	Disabled	—	Disabled	—	NA	NA	Enabled	1G	N	N	N
	.3at	25.5	30	2X2	23	2X2	23	NA	NA	Enabled	1G	N	Y	N
	.3bt / UPOE / DC	33.6	39.5	4X4	24	4X4	24	NA	NA	Enabled	2.5G	Y	Y	N
	.3bt / UPOE / DC	51	60	4X4	24	4X4	24	NA	NA	Enabled	2.5G	Y	Y	Y

Access Points	PoE Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode										
		at AP	Worst-Case Cable	Radio 0	R0 dBm Per Path	Radio 1	R1 dBm Per Path	Radio 2	R02 dBm Per Path	AUX Radio	Ethernet Mgig	SFP Module	GbE PHY	REOt
				2.4 GHz Radio		5 GHz Primary Radio		5 GHz Secondary Radio		Ohvae				
Cisco Catalyst 9124 AXI Cisco Catalyst 9124 AXD Single 5G Radio	.3at	25.5	30	Shutdown	—	4X4	24	Shutdown	—	Enabled	2.5G	Y	N	N
Cisco Catalyst 9124 AXE TriRadio Mode	.3af	13.8	15.4	Disabled	—	Disabled	—	Disabled	—	Enabled	1G	N	N	N
	.3at	25.5	30	Disabled	—	Disabled	—	Disabled	—	Enabled	1G	N	N	N
	.3bt / UPOE / DC	33.6	39.5	2X2	24	2X2	24	2X2	24	Enabled	2.5G	Y	Y	N
	.3bt / UPOE / DC	51	60	2X2	24	2X2	24	2X2	24	Enabled	2.5G	Y	Y	Y
Cisco Catalyst 9124 AXE Dual 5G Radio	.3at	25.5	30	Shutdown	—	2X2	23	2X2	23	Enabled	1G	N	Y	N

Wakeup Threshold for Access Point Power Save Mode

The Wakeup Threshold feature enables you to define the client threshold in the AP power profile configuration to determine when the AP wakes up from the power save mode or enter into the power save mode.

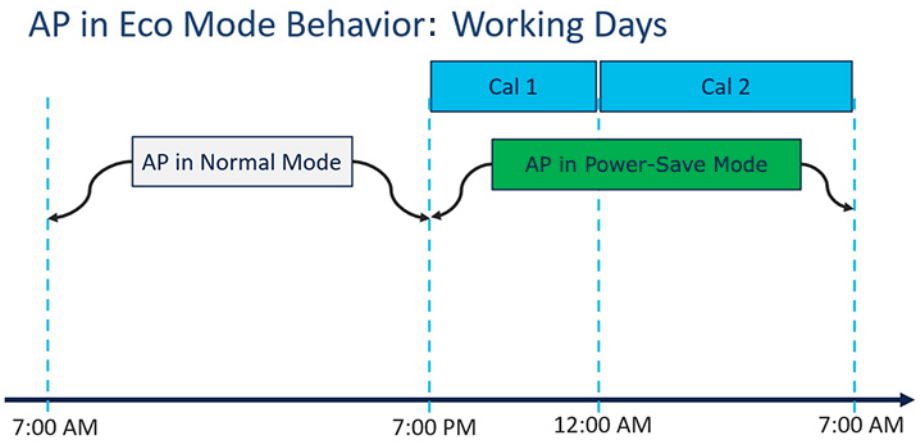
When the AP applies the calendar associated power profile (for an active calendar), and the number of connected clients reach the wakeup threshold, the AP wakes up from power save mode and goes into the Fixed power profile mode or the Regular power profile (insufficient power) mode.

When the AP applies the calendar associated power profile (for an active calendar), and the number of connected clients is less than the wakeup threshold, the AP applies the calendar associated power profile to shut down the interface or to lower the interface speed to save power.

AP Power Save Scenarios

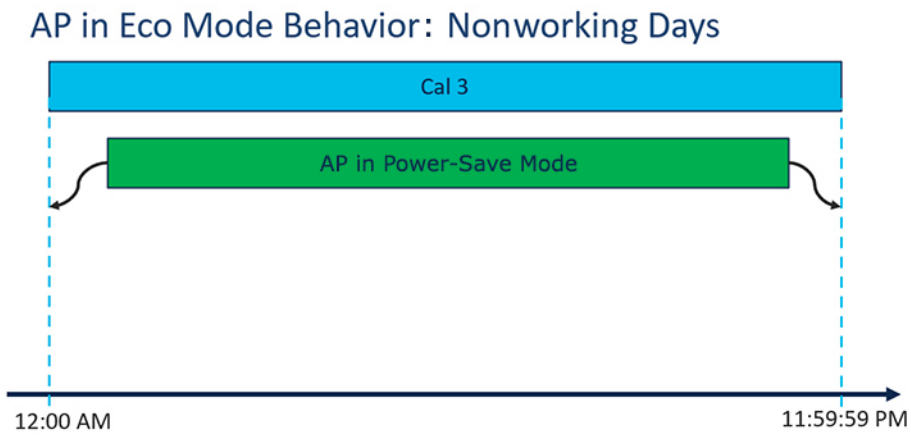
The AP Power Save feature helps APs to enter into a power-save mode or low-power mode by applying a calendar, for example, for after hours, associated with the corresponding power profile. The AP profile is enhanced to associate a PoE power policy with calendar profiles. The following are the scenarios for Eco mode APs:

- ***Figure 18: AP in Eco Mode Behavior: Working Days***



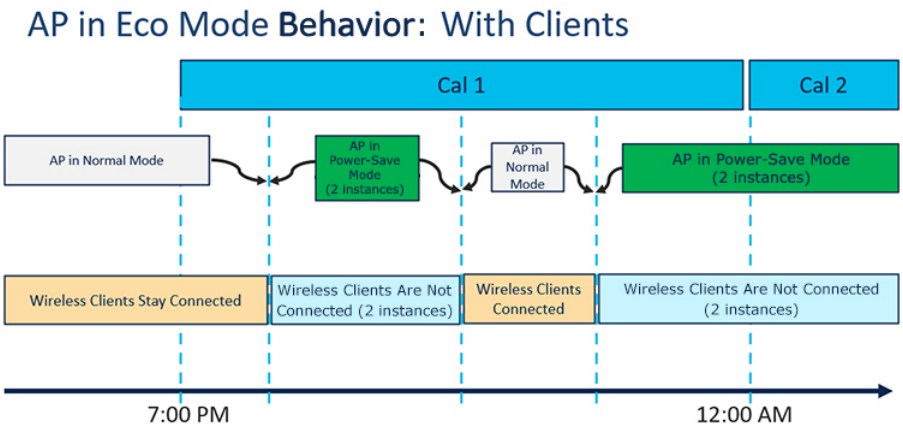
On working days, from 7:00 a.m. to 7:00 p.m, the AP functions in normal mode or fixed mode, when the maximum number of clients are connected to the AP. From 7:00 p.m. to 12:00 a.m., the **Cal1** calendar profile timer starts to put the AP in the power-save mode. Likewise, the **Cal2** calendar profile timer starts, and extends the power-save mode from 12:00 a.m. to 7:00 a.m. Again, at 7:00 a.m., the AP goes into normal mode.

- *Figure 19: AP in Eco Mode Behavior: Nonworking Days*



On nonworking days, the AP goes into power-saving mode from 12:00 a.m. to 11:59:59 p.m. The **Cal3** calendar profile is applied here. This profile defines the timer for the power-save mode. This means that there are no clients connected to the AP, and that the AP is asleep.

- *Figure 20: AP in Eco Mode Behavior: With Clients*



When clients are connected to the AP, the AP automatically switches to the normal mode. For example, in the calendar profile **Cal1**, the AP is in normal mode, because wireless clients are connected to the AP. At 8:00 p.m., clients get dissociated from the AP, and the AP goes into power-save mode. When clients enter the AP coverage area at 9:30 p.m., the AP automatically switches from power-save mode to normal mode of operation.

Configuring Power Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Power Profile**.

Step 2 Click **Add**.
The **Add Power Profile** window is displayed.

Step 3 Enter a name and description for the power profile. The name must be ASCII characters of up to 128 characters, without leading or trailing spaces.

Step 4 Click **Add** to add rules for the power profile.

Step 5 In the **Sequence number** field, enter a unique sequence number to designate the priority in which power should be disabled for the component. The sequence number of 0 indicates that the component should be disabled first.

Step 6 From the **Interface** and **Interface ID** drop-down list, choose interface and interface ID to designate to the component for which the power derating rule applies.

Step 7 From the **Parameter** and **Parameter value** drop-down list, choose the values depending on the interface you chose in step 6.

For example, if you chose **Ethernet** as an interface, you can further customize the rule for the interface by choosing the associated speed. This rule ensures that the AP disables power for the Ethernet interface that is operating at a higher speed, and thereby consuming more power.

Step 8 Click the check mark to save and then click **Apply to Device**.

Configuring a Power Policy Profile (CLI)

Before you begin

You must keep at least one radio interface up and running before you configure a power policy profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile power** *power-profile-name* **Example:** `Device(config)# wireless profile power power-profile-name`	Configures the power policy profile.

	Command or Action	Purpose
Step 3	*sequence-number* **ethernet** {**GigabitEthernet0** | **GigabitEthernet1 speed** {**1000mbps** | **100mbps** | **2500mbps** | **5000mbps**} | **LAN1** | **LAN2** | **LAN3 state disable**} **Example:** `Device(config-wireless-power-profile)# 10 ethernet gigabitethernet1 speed 1000mbps`	Configures the power policy for Ethernet. *sequence-number*: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values, however, the parameter value that yields the lowest power consumption is the one that gets selected, irrespective of the sequence number if there is active calendar. **Note** • The Ethernet interface is used to join the controller. The uplink interface is not disabled even if it is defined in the power policy. • Ethernet speed configuration is not operational in Cisco IOS XE 17.8.1 and later releases.
Step 4	*sequence-number* **radio 24ghz** {**spatial-stream** {**1** | **2** | **3** | **4**} | **state shutdown**} **Example:** `Device(config-wireless-power-profile)# 20 radio 24ghz spatial stream 2`	Configures spatail stream for the 2.4-GHz band radio. Here: *sequence-number*: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values. • 1: Specifies a 1X1 radio spatial stream. • 2 : Specifies a 2X2 radio spatial stream. • 3 : Specifies a 3X3 radio spatial stream. • 4 : Specifies a 4X4 radio spatial stream. **state shutdown**: Indicates that the radio state is down.
Step 5	*sequence-number* **radio 5ghz** {**spatial-stream** {**1** | **2** | **3** | **4** | **8**} | **state shutdown**}	Configures spatail stream for the 5-GHz band radio.

	Command or Action	Purpose
	Example: `Device(config-wireless-power-profile)# 30 radio 5ghz spatial stream 4`	Here: *sequence-number*: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values. • 1: Specifies a 1X1 radio spatial stream. • 2 : Specifies a 2X2 radio spatial stream. • 3 : Specifies a 3X3 radio spatial stream. • 4 : Specifies a 4X4 radio spatial stream. • 8 : Specifies a 8X8 radio spatial stream. **state shutdown**: Indicates that the radio state is down.
Step 6	*sequence-number* **radio secondary-5ghz** {**spatial-stream** {**1** | **2** | **3** | **4** | **8**} | **state shutdown**} **Example:** `Device(config-wireless-power-profile)# 40 radio 5ghz spatial stream 4`	Configures spatail stream for a secondary 5-GHz band radio. Here: *sequence-number*: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values. • 1: Specifies a 1X1 radio spatial stream. • 2 : Specifies a 2X2 radio spatial stream. • 3 : Specifies a 3X3 radio spatial stream. • 4 : Specifies a 4X4 radio spatial stream. • 8 : Specifies a 8X8 radio spatial stream. **state shutdown**: Indicates that the radio state is down.
Step 7	*sequence-number* **radio 6ghz** {**spatial-stream** {**1** | **2** | **3** | **4** | **8**} | **state shutdown**} **Example:**	Configures spatail stream for the 6-GHz band radio. Here:

	Command or Action	Purpose
	`Device(config-wireless-power-profile)# 50 radio 6ghz spatial stream 2`	*sequence-number*: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values. • 1: Specifies a 1X1 radio spatial stream. • 2 : Specifies a 2X2 radio spatial stream. • 3 : Specifies a 3X3 radio spatial stream. • 4 : Specifies a 4X4 radio spatial stream. • 8 : Specifies a 8X8 radio spatial stream. **state shutdown**: Indicates that the radio state is down.
Step 8	*sequence-number* **usb 0 state disable** **Example:** `Device(config-wireless-power-profile)# 60 usb 0 state disable`	Configures the power policy for USB.

Configuring a Calendar Profile (GUI)

Configure calendar profiles to set up a daily, weekly, or monthly recurrence schedule.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Calendar**.

Step 2 Click **Add**.
The **Add Calendar Profile** window is displayed.

Step 3 Enter a name for the calendar profile. The name must be ASCII characters of up to 32 characters, without leading or trailing spaces.

Step 4 From the **Recurrence** drop-down list, choose the schedule for which you want to create a profile.

Step 5 Select the **Start Time** and the **End Time** for the recurrence schedule.

Note

- For daily recurrences, you can select the start time and end time. For example, if you want the AP to derate the power on certain interfaces between 7 p.m. to 7 a.m. daily, or if you want the controller to not allow any clients to be associated during this period, you can set up this daily recurrence schedule.

  To cover this timespan, you must create two calendar profiles, one for 7 p.m. till 23:59:59, and another one from midnight to 7 a.m. of the next calendar day, and map it to the same power profile. After this, assign it to the AP Join profile.

- For weekly recurrences, select the specific days of the week along with the start and end time.
- For monthly recurrence, select the specific days of the month along with the start and end time.

Step 6 Click **Apply** to save the configuration.

Configuring a Calendar Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile calendar-profile name** *calendar_profile_ap_power* **Example:** `Device# wireless profile calendar-profile name ap_power_calendar`	Configures a calendar profile. Enters the calendar profile configuration mode. Here, **name** refers to the name of the calendar profile.
Step 3	**recurrence daily** **Example:** `Device(config-calendar-profile)# recurrence daily`	Configures daily recurrence for daily profile.
Step 4	**start** *start-time* **end** *end-time* **Example:** `Device(config-calendar-profile)# start 16:00:00 end 20:00:00`	Configures the start time and end time for calendar profile.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-calendar-profile)# end`	

Configuring a Power Policy in an AP Join Profile (GUI)

Power policy supports the use of a power profile or a mapped configuration of a power profile and a calendar profile that are pushed to an AP during an AP join session. You can map a maximum of five combination profiles (calendar and power) per AP profile.

Before you begin

Ensure that the power profile and calendar profile are created and displayed in the respective drop-down lists in the GUI.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.
The **Add AP Join Profile** window is displayed.

Step 2 Click the **AP** tab.

Step 3 Under the AP tab, click the **Power Management** tab.

Step 4 From the **Regular Power Profile** drop-down list, choose the power profile.
The AP applies these settings to derate the power based on the configured priority list.

Note If you want the AP to apply the power profile configuration during a specific time period, choose the **Calendar Profile** and map it to the power profile from the drop-down list.

Step 5 Click the check mark to associate the mapping.

Step 6 Click **Apply to Device** to save the configuration.

Mapping a Power Profile Under an AP Profile (CLI)

Before you begin

Ensure that you have defined a calendar profile in the wireless profile, before you map the calendar profile to an AP join profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**power-profile** *power-profile-name* **Example:** `Device(config-ap-profile)# power-profile power-profile-name`	Configures the AP power profile. This power profile is used during non-calendar hours to meet the power budget provided by the switch connected to the AP.
Step 4	**calendar-profile** *calendar-profile-name* **Example:** `Device(config-ap-profile)# calendar-profile ap-calendar-profile`	Maps a calendar profile to the AP profile. Enters the AP profile calendar configuration mode.
Step 5	**[no] action power-saving-mode power-profile** *power-profile-name* **Example:** `Device(config-ap-profile-calendar)# action power-saving-mode power-profile power-profile1`	Maps a specific power profile to a specific calendar profile. Maps the power-saving mode action for the calendar profile. Use the **no** form of this command to disable the command. **Note** You can have more than one mapping of calendar profile to power profile.

Configuring Client Wakeup Threshold (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile power** *power-profile-name* **Example:** `Device(config)# wireless profile power power-profile1`	Configures the power policy profile.
Step 3	**power-save-client-threshold** *client-threshold* **Example:** `Device(config-wireless-power-profile)# power-save-client-threshold 5`	Configures the client threshold up to which the AP can stay in the power save mode. The valid range is between 1 and 32 clients. The default value is 1.

Configuring PoE-Out Interface in Power Profile (GUI)

Before you begin

Enable the RLAN port for the AP.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Power Profile**.

Step 2 Click **Add**.
The **Add Power Profile** window is displayed.

Step 3 Enter a name and description for the power profile. The name can contain up to 128 ASCII characters, without leading or trailing spaces.

Step 4 (Optional) From the **Power Save Client Threshold** counter, select a value to set a limit to the number of client associations with the AP. The default value is 1. The valid range is between 1 to 32.

Step 5 Click **Add** to create a rule for the PoE-Out interface.
The **Rule** section is displayed in the window.

Step 6 In the **Rule** section, complete the following steps:

a) In the **Sequence number** field, enter a unique sequence number to assign the priority in which power should be disabled for the component. A sequence number of 0 indicates that the component should be disabled first.
b) From the **Interface** drop-down list, choose **Ethernet** as the interface.
c) From the **Interface ID** drop-down list, choose one of the following interfaces: **LAN1**, **LAN2**, or **LAN3**.
d) From the **Parameter** drop-down list, choose **POE-out**.

A POE-out port on an AP is used to provide power to the another device, for example, a camera. This selection ensures that the power usage of the port is reduced or shut down at the specified sequence.

Step 7 Click the check mark button to save.

Step 8 Click **Apply to Device**.

Configuring PoE-Out Interface in Power Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile power** *power-profile-name* **Example:** `Device(config)# wireless profile power poe-out-power-profile`	Configures the power policy profile. Enters the wireless power profile configuration mode.
Step 3	*sequence-number* **ethernet LAN1 poe-out disable** **Example:** `Device(config-wireless-power-profile)# 1 ethernet LAN1 poe-out disable`	Disables the PoE-out state.

Configuration Example of Power Profile

The following example shows how to define a power save policy:

```
wireless profile power power-save
            10 radio 5ghz state shutdown
            20 radio secondary-5ghz state shutdown
            30 radio 6ghz state shutdown
            40 usb 0 state disable
```

The following example shows how to define a calendar profile:

```
wireless profile calender-profile name eve-to-midnight
            recurrence daily
            start 19:00:00 end 23:59:59
wireless profile calender-profile name midnight-to-morning
            recurrence daily
            start 00:00:00 end 07:00:00
wireless profile calender-profile name weekends
            recurrence weekly
            day Saturday
            day Sunday
            start 00:00:00 end 23:59:59
```

The following example shows how to define an AP join profile and map a calendar profile to a power profile:

```
ap profile wireless-prof-site1
                 calendar-profile eve-to-midnight
                  action power-saving-mode power-profile power-save
                 calendar-profile midnight-to-morning
                  action power-saving-mode power-profile power-save
                 calendar-profile weekends
                  action power-saving-mode power-profile power-save
```

Verifying Access Point Power Policy (GUI)

To verify the applied configuration on the GUI, follow these steps:

Procedure

Step 1 Choose **Monitoring** > **AP Statistics**.

Step 2 Click a Cisco Catalyst 9136 series AP from the list of APs.
The **General** window is displayed.

Step 3 Click the **Power** tab.
The **Power Operational Status** and the **AP Fixed Power Policy** details are displayed.

Step 4 Click **OK**.

To verify the AP fixed power policy details from the list of configured APs, follow these steps:

Procedure

Step 1 Choose **Configuration** > **Access Points**.

Step 2 Click a Cisco Catalyst 9136 series AP from the list of APs.
The **Edit AP** window is displayed.

Step 3 Click the **Interfaces** tab.
The **AP Fixed Power Policy** details are displayed.

Step 4 Click **Update & Apply**.

Verifying the Access Point Power Profile

To view the calendar profile and its mapping, run the following command:

```
Device# show ap profile name default-ap-profile detailed
AP Profile Name                      : default-ap-profile
Description                          : default ap profile
Power profile name                   : power_prof_day
AP packet capture profile            : Not Configured
AP trace profile                     : Not Configured
Mesh profile name                    : default-mesh-profile
Power profile name                   : Not Configured
Calendar Profile
    Profile Name                    : cal47
    Power saving mode profile name : pow_da
    ---------------------------------------------------
    Profile Name                    : cal48
    Power saving mode profile name : pow23
    ---------------------------------------------------
```

To view the operational details of the AP, run the following command:

```
Device# show ap name cisco-ap power-profile summary
AP power derate Capability      : Capable

Power saving mode
Power saving mode profile        : pow2
Associated calendar profile      : cal1

AP power profile status         : Insufficient De-rating
```

```
Interface    Interface-ID       Parameter        Parameter value    Status
-------------------------------------------------------------------------------------
Radio        5 GHz              State            DISABLED           Success
Radio        6 GHz              State            DISABLED           Not Applicable
Ethernet     LAN1               State            DISABLED           Not Applicable
Radio        2.4 GHz            State            DISABLED           Success
Ethernet     Gig0               Speed            5000 MBPS          Fixed Policy
```

AP power derate capability is displayed in the output as **Capable** only for those APs that support power policy. For the other APs, it is displayed as **Not Capable**.

In the **show ap name cisco-ap power-profile summary** output, in the power saving mode, the status of the interface configured in the power profile (for example, **pow2**) is applied on the AP, and the AP sends the details (that are displayed in the show command) such as, the name of the power saving profile and the associated calendar profile.

The table that is displayed shows the interfaces and the parameter status of the power saving profile. The AP sends the information as to which of the interfaces are disabled. For example, if the AP does not have a 6-GHz radio interface, the **Status** is displayed as **Not Applicable**. If the interfaces are applied without any errors, then **Success** is displayed.

Note When the AP uses the fixed power policy, due to inactive calendar or client connectivity, the interfaces are not displayed in the power profile summary if their status is UP on the AP.

Verifying Radio Spatial Streams

To view the configuration and operational details of radio spatial stream rules in the power profile, run the following commands:

```
Device# show wireless profile power detailed wireless_pow_profile_name
Power profile name             : wireless_pow_profile_name
-----------------------------------------------
Description                    :
.
.
Seq No       Interface    Interface-id       Parameter        Parameter value
-------------------------------------------------------------------------------
100          Radio        6 GHz              Spatial Stream   2 x 2
200          Radio        5 GHz              Spatial Stream   8 x 8
400          USB          USB0               State            DISABLED
500          Ethernet     Gig0               Speed            100 MBPS
600          Radio        6 GHz              State            DISABLED
700          Radio        2.4 GHz            State            DISABLED
900          Radio        5 GHz              State            DISABLED
```

```
Device# show ap name cisco-ap-name power-profile summary
AP power derate Capability      : Capable

AP fixed power policy
---------------------

Interface    Interface-ID       Parameter        Parameter value    Status
-------------------------------------------------------------------------------------
Ethernet     Gig0               Speed            5000 MBPS          Fixed Policy
Radio        2.4 GHz            Spatial Stream   4 x 4              Fixed Policy
Radio        5 GHz              Spatial Stream   8 x 8              Fixed Policy
```

```
Radio        Sec 5 GHz          Spatial Stream   4 x 4              Fixed Policy
USB          USB0               State            DISABLED           Fixed Policy
```

Verifying Client Threshold

To view the client threshold details, run the following command:

```
Device# show wireless profile power detailed profile1
Power profile name             : profile1
-----------------------------------------------
Description                    : Power profile 1
Power save client threshold    : 5
Seq No       Interface    Interface-id       Parameter        Parameter value
-------------------------------------------------------------------------------
0             Radio        6 GHz             State              DISABLED
1             Radio        5 GHz             Spatial Stream     1 x 1
2             Radio        2.4 GHz           Spatial Stream     2 x 2
3             USB          USB0              State              DISABLED
```

Verifying PoE-Out Details

To view the PoE-out details in the wireless power profile, run the following commands:

```
Device# show wireless profile power detailed poe-out_profile_name
Power profile name             : poe-out_profile_name
-----------------------------------------------
Description                    : profile-description
Seq No       Interface    Interface-id       Parameter        Parameter value
-------------------------------------------------------------------------------
10 ...
20           Ethernet     LAN 1              POE_OUT          DISABLED
30 ...
```

```
Device# show ap name Cisco-Ap1 power-profile summary
AP power derate Capability      : Capable

AP fixed power policy
---------------------

Interface    Interface-ID       Parameter        Parameter value    Status
-----------------------------------------------------------------------------------------
...
Ethernet     LAN 1              POE_OUT          DISABLED           Fixed Policy
...
```

Information About Access Point Real-Time Statistics

From Cisco IOS XE Bengaluru 17.5.1 onwards, you can track the CPU utilization and memory usage of an AP, and monitor the health of an AP, by generating real-time statistics for an AP.

SNMP traps are defined for CPU and memory utilization of APs and the controller. An SNMP trap is sent out when the threshold is crossed. The sampling period and statistics interval can be configured using SNMP, YANG, and CLI.

Statistics interval is used to process the data coming from an AP, and the average CPU utilization and memory utilization is computed over time. You can also configure an upper threshold for these statistics. When a statistic value surpasses the upper threshold, an alarm is enabled, and an SNMP trap is triggered.

From Cisco IOS XE Cupertino 17.7.1 release onwards, for radio monitoring, you can reset the radios based on the statistics sent by the AP for a sampling period. When you configure the radios in the controller, if there is no increment in the Tx or Rx statistics when the radio is up, then the radio reset is triggered.

Feature History for Real Time Access Point Statistics

This table provides release and related information for the feature explained in this module.

Table 35: Feature History for Real Time Access Point Statistics

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.7.1	Real Time Access Point Statistics	This feature is enhanced with the implementation of AP threshold values between 0 and 50 to trigger an alarm.

Restrictions for AP Radio Monitoring Statistics

You cannot reset the radio firmware from the controller. The controller will shut and unshut the radio if the Rx or Tx count is not incremented for a radio slot in a specified period.

Configuring Access Point Real Time Statistics (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > AP Join**.

Step 2 Click **Add**. The **Add AP Join Profile** page is displayed.

Step 3 Under the **AP** tab, click the **AP Statistics** tab.

Step 4 In the **System Monitoring** section:

a) Enable **Monitor Real Time Statistics** to get calculated statistics and alarms of the AP.

b) To receive an alarm when the upper threshold is surpassed for parameters such as CPU utilization and memory, enable **Trigger Alarm for AP**.

c) Enter the threshold percentage for CPU and memory usage in the **CPU Threshold to Trigger Alarm** field and **Memory Threshold to Trigger Alarm** fields, respectively. The valid range is between 0 to 50. An SNMP trap is sent out when this threshold is crossed.

d) In the **Interval to Hold Alarm** field, enter the time for which the alarm is held before it gets triggered. The valid range is between 0 and 3600 seconds.

e) In the **Trap Retransmission Time** field, enter the time between retransmissions of the alarm. The valid range is between 0 and 65535 seconds.

f) To define how often data should be collected from the AP, enter a value in the **Sampling Interval** field. The valid range is between 720 and 3600 seconds.

g) To define the interval at which AP statistics are to be calculated, enter a value in the **Statistics Interval** field. The valid range is between 2 and 900 seconds.

h) To automatically reload the AP when there is high CPU and memory usage in the defined sampling interval, select the **Reload the AP** check box.

Step 5 Under the **Radio Monitoring** section:

a) Select the **Monitoring of AP Radio stuck** check box to verify that the Tx and Rx statistics of the AP are updated each time the payloads are coming in from the AP to the controller.

b) To generate an alarm for the radio of the AP when there is no increment in the Tx and RX statistics for the payloads, select the **Alarms for AP Radio stuck** check box.

c) Select the **Reset the stuck AP Radio** check box to recover the radio from the bad state. A radio admin state payload will be sent from the controller to toggle the radio and the radio will be shut when there is no increment in the Tx and Rx statistics.

d) To define how often data should be collected from the radio, enter a value in the **Sampling Interval** field. The valid range is between 720 and 3600 seconds.

Step 6 Click **Apply to Device** to save the configuration.

Configuring Real-Time Access Point Statistics (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile doc-test`	Configures the AP profile. The default AP join profile name is *default-ap-profile*.
Step 3	**stats-timer** *frequency* **Example:** `Device(config-ap-profile)# stats-timer 60`	(Optional) Configures the statistics timer. This command is used to change the frequency of the statistics reports coming from the AP. The valid values range between 0 and 65535 seconds.
Step 4	**statistics ap-system-monitoring enable** **Example:** `Device(config-ap-profile)# statistics ap-system-monitoring enable`	(Optional) Enables monitoring of AP real-time statistics (CPU and memory).

	Command or Action	Purpose
Step 5	**statistics ap-system-monitoring alarm-enable** **Example:** `Device(config-ap-profile)# statistics ap-system-monitoring alarm-enable`	Enables alarms for AP real-time statistics (CPU and memory).
Step 6	**statistics ap-system-monitoring alarm-hold-time** *duration* **Example:** `Device(config-ap-profile)# statistics ap-system-monitoring alarm-hold-time 400`	Defines the alarms for AP real-time statistics (CPU and Memory). The valid values range between 0 and 3600 seconds.
Step 7	**ap-system-monitoring alarm-retransmit-time** *duration* **Example:** `Device(config-ap-profile)# ap-system-monitoring alarm-retransmit-time 100`	Defines the interval between retransmissions of the trap alarm. The valid values range between 0 and 65535 seconds.
Step 8	**statistics ap-system-monitoring cpu-threshold** *percentage* **Example:** `Device(config-ap-profile)# statistics ap-system-monitoring cpu-threshold 30`	Defines the threshold for CPU usage on the AP (percentage) to trigger alarms. **Note** From Cisco IOS XE Cupertino 17.7.1 release onwards, the valid threshold value for CPU on the AP to trigger the alarms is between 0 and 50.
Step 9	**ap-system-monitoring mem-threshold** *percentage* **Example:** `Device(config-ap-profile)# ap-system-monitoring mem-threshold 40`	Defines the threshold for memory usage on AP to trigger alarms. The percentage of threshold for memory usage on the AP to trigger is between 0 and 100. **Note** From Cisco IOS XE Cupertino 17.7.1 release onwards, the valid threshold value for memory usage on the AP to trigger the alarms is between 0 and 50.
Step 10	**ap-system-monitoring sampling-interval** *duration* **Example:** `Device(config-ap-profile)# statistics ap-system-monitoring sampling-interval 600`	(Optional) Defines the sampling interval. The valid values range between 2 and 900 seconds.
Step 11	**exit** **Example:**	Exits from AP profile configuration mode and returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-ap-profile)# exit`	
Step 12	**trapflags ap ap-stats** **Example:** `Device(config)# trapflags ap ap-stats`	Enables sending AP-related traps. Traps are sent when statistics exceed the configured threshold.

Example

```
Device(config)# ap profile default-policy-profile
Device(config-ap-profile)# statistics ap-system-monitoring enable
Device(config-ap-profile)#statistics ap-system-monitoring sampling-interval 90
Device(config-ap-profile)#statistics ap-system-monitoring stats-interval 120
Device(config-ap-profile)#statistics ap-system-monitoring alarm-enable
Device(config-ap-profile)#statistics ap-system-monitoring alarm-hold-time 3
Device(config-ap-profile)#statistics ap-system-monitoring alarm-retransmit-time 10
Device(config-ap-profile)#statistics ap-system-monitoring cpu-threshold 90
Device(config-ap-profile)#statistics ap-system-monitoring mem-threshold 90
Device(config)# trapflags ap ap-stats
```

Configuring AP Radio Monitoring Statistics

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile test1`	Configures an AP profile and enters the AP profile configuration mode.
Step 3	**statistic ap-radio-monitoring enable** **Example:** `(config-ap-profile)#statistic ap-radio-monitoring enable`	Enables the monitoring of AP radio stuck statistics.
Step 4	**statistic ap-radio-monitoring alarm-enable** **Example:** `(config-ap-profile)#statistic ap-radio-monitoring alarm-enable`	(Optional) Enables the alarm for AP radio stuck statistics.
Step 5	**statistic ap-system-monitoring action reload-ap interval** *duration* **Example:**	(Optional) Specifies the sampling interval in seconds. The valid values range between 720 and 3600 seconds.

	Command or Action	Purpose
	`(config-ap-profile)# statistic ap-radio-monitoring action reload-ap interval850`	
Step 6	**statistic ap-radio-monitoring action radio-reset** **Example:** `(config-ap-profile)# statistic ap-radio-monitoring action radio-reset`	(Optional) Generates an alarm and resets the radio if the radio is stuck.
Step 7	**statistic ap-system-monitoring action reload-ap** **Example:** `(config-ap-profile)# statistic ap-system-monitoring action reload-ap`	Reloads the AP.

Example

```
Device(config)# ap profile test1
Device(config-ap-profile)# statistics ap-radio-monitoring enable
Device(config-ap-profile)#statistic ap-radio-monitoring alarm-enable
Device(config-ap-profile)#statistic ap-radio-monitoring sampling-interval 750
Device(config-ap-profile)# statistic ap-radio-monitoring action radio-reset
Device(config-ap-profile)#statistic ap-system-monitoring action reload-ap
```

Monitoring Access Point Real-Time Statistics (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **AP Statistics**.

Step 2 Click the **General** tab.

Step 3 Click an AP name. The **General** window is displayed.

Step 4 To view the AP Statistics data, click the **AP Statistics** tab.

The following information is displayed:

- **Memory alarm last send time**: Displays the time of the last memory trap sent.
- **Memory Alarm Status**: Displays the state of the memory alarm. An alarm can be **ACTIVE**, **INACTIVE**, **INACTIVE_SOAKING**, **ACTIVE_SOAKING**. An alarm is soaked until the configured hold time has passed.
- **Memory alarm raise time**: Displays the last time the memory alarm was active.
- **Memory alarm clear time**: Displays the last time the memory alarm was inactive.

- **Last statistics received**: Displays the time of the last statistics report received from the AP.
- **Current CPU Usage**: Displays the latest percentage of CPU usage reported.
- **Average CPU Usage**: Displays the average CPU usage calculated.
- **Current Memory Usage**: Displays the latest percentage of memory usage reported.
- **Average Memory Usage**: Displays the average memory usage calculated.
- **Current window size**: Displays the window size. The window size is calculated by dividing the statistics interval by the sampling interval. The average CPU and memory usage is calculated by the window size.
- **CPU alarm last send time**: Displays the time of the last CPU trap sent.
- **CPU Alarm Status**: Displays the state of the CPU alarm. An alarm can be **ACTIVE**, **INACTIVE**, **INACTIVE_SOAKING**, **ACTIVE_SOAKING**. An alarm is soaked until the configured hold time has passed.
- **CPU alarm raise time**: Displays the last time the CPU alarm was active.
- **CPU alarm clear time**: Displays the last time the CPU alarm was inactive.

Step 5 Click **OK**.

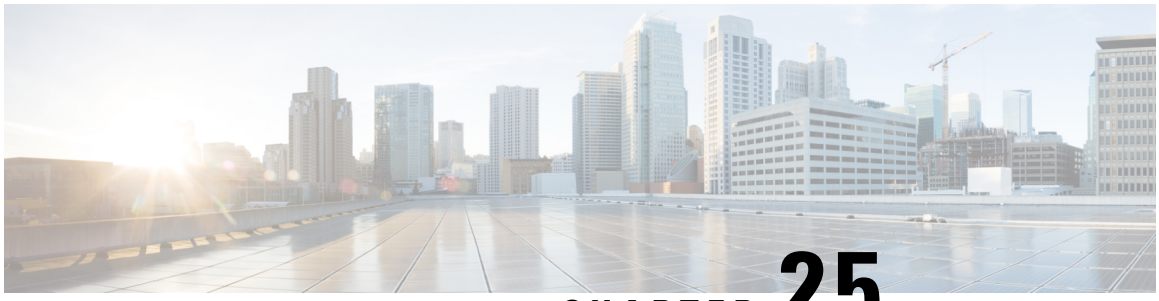
Verifying Access Point Real-Time Statistics

To verify AP real-time statistics, run the **show ap config general | section AP statistics** command:

```
Device# show ap config general | section AP statistics
!Last Statistics
AP statistics : Enabled
Current CPU usage : 4
Average CPU usage : 49
Current memory usage : 35
Average memory usage : 35
Last statistics received : 03/09/2021 15:25:08
!Statistics Configuration
Current window size : 1
Sampling interval : 30
Statistics interval : 300
AP statistics alarms : Enabled
!Alarm State - Active, Inactive, Inactive_Soaking, Inactive_Soaking
Memory alarm status : Active
Memory alarm raise time : 03/09/2021 15:24:29
Memory alarm clear time : NA
Memory alarm last send time : 03/09/2021 15:24:59
CPU alarm status : Inactive
CPU alarm raise time : 03/09/2021 15:24:25
CPU alarm clear time : 03/09/2021 15:25:05
CPU alarm last send time : 03/09/2021 15:25:05
!Alarm Configuration
Alarm hold time : 6
Alarm retransmission time : 30
Alarm threshold cpu : 30
Alarm threshold memory : 32
```

To verify the statistics reporting period, run the **show ap config general | i Stats Reporting Period** command:

```
Device# show ap config general | i Stats Reporting Period
Stats Reporting Period : 10
```



CHAPTER 25

AP Configuration

- Feature History for Configuring the Access Point Console, on page 446
- Information About Configuring the Access Point Console, on page 446
- Configuring the AP Console (GUI), on page 447
- Configuring the AP Console (CLI), on page 447
- Verifying the AP Console Status, on page 447
- Information About AP Audit Configuration, on page 448
- Restrictions for AP Audit Configuration, on page 448
- Configure AP Audit Parameters (CLI), on page 449
- Verifying AP Audit Report Summary, on page 449
- Verifying AP Audit Report Detail, on page 449
- 2.4-GHz Radio Support, on page 450
- 5-GHz Radio Support, on page 452
- 6-GHz Radio Support, on page 455
- Information About Dual-Band Radio Support , on page 457
- Configuring Default XOR Radio Support, on page 458
- Configuring XOR Radio Support for the Specified Slot Number (GUI), on page 460
- Configuring XOR Radio Support for the Specified Slot Number, on page 461
- Receiver Only Dual-Band Radio Support, on page 463
- Configuring Client Steering (CLI), on page 464
- Verifying Cisco Access Points with Dual-Band Radios, on page 466
- Information About OFDMA Support for 11ax Access Points, on page 466
- Configuring 11AX (GUI), on page 467
- Configuring Channel Width, on page 467
- Configuring 802.11ax Radio Parameters (GUI), on page 468
- Configuring 802.11ax Radio Parameters (CLI), on page 468
- Setting up the 802.11ax Radio Parameters, on page 469
- Configuring OFDMA on a WLAN, on page 470
- Verifying Channel Width, on page 471
- Verifying Client Details, on page 472
- Verifying Radio Configuration, on page 473
- Information About Cisco Flexible Antenna Port, on page 476
- Configuring a Cisco Flexible Antenna Port (GUI), on page 476
- Configuring a Cisco Flexible Antenna Port (CLI), on page 476

• Verifying Flexible Antenna Port Configuration, on page 477
• Feature History for Environmental Sensors in Access Points, on page 477
• Information About Environmental Sensors in Access Points, on page 478
• Use Cases, on page 478
• Configuring Environmental Sensors in an AP Profile (CLI), on page 478
• Configuring Environment Sensors in Privileged EXEC Mode (CLI), on page 479
• Verifying the AP Sensor Status, on page 480
• Information About CAPWAP LAG Support, on page 480
• Restrictions for CAPWAP LAG Support, on page 481
• Enabling CAPWAP LAG Support on Controller (GUI), on page 481
• Enabling CAPWAP LAG Support on Controller, on page 482
• Enabling CAPWAP LAG Globally on Controller, on page 482
• Disabling CAPWAP LAG Globally on Controller, on page 482
• Enabling CAPWAP LAG for an AP Profile (GUI), on page 483
• Enabling CAPWAP LAG for an AP Profile, on page 483
• Disabling CAPWAP LAG for an AP Profile, on page 484
• Disabling CAPWAP LAG Support on Controller , on page 484
• Verifying CAPWAP LAG Support Configurations, on page 485

Feature History for Configuring the Access Point Console

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 36: Feature History for Configuring the Access Point Console

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	Configuring the Access Point Console	This feature allows you to configure the Access Point (AP) console from the controller. In Cisco IOS XE Cupertino 17.8.x and earlier releases, the AP console could be disabled from the controller, only by enabling the Federal Information Processing Standard (FIPS) mode or the Common Criteria (CC) mode.

Information About Configuring the Access Point Console

From Cisco IOS XE Cupertino 17.9.1 onwards, a new option (a configuration knob) is introduced to enable the Access Point console from the controller, which is independent of the FIPS mode or the high-security mode (CC mode). (Until Cisco IOS XE Cupertino 17.8.1, the console was enabled by default). This configuration knob can be activated through the controller GUI and CLI.

Console enablement is isolated from the FIPS mode and is configured through the AP join profile. In the CC mode, the console and SSH are disabled. When you enable the CC mode, it overrides the AP console configurations, if any, done from the AP profile.

Configuring the AP Console (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 In the **Management** tab, in the **Telnet/SSH Configuration** section, check the **Serial Console** check box.

Step 3 Click **Apply to Device**.

Configuring the AP Console (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**[no] console** **Example:** `Device(config-ap-profile)# console`	Enables the AP serial console port. Use the **no** form of this command to disable the AP serial console port.

Verifying the AP Console Status

To verify the AP console status from the controller, run the following command:

```
Device# show ap config general | include ap-Name | console
Cisco AP Name : CiscoAP
================================================

Cisco AP Identifier : 6XXX.bXXX.aXXX
Country Code : US
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-AB 802.11 6GHz:-B
AP Country Code : US - United States
AP Regulatory Domain
802.11bg : -A
802.11a : -B
MAC Address : 6XXX.bXXX.0XXX
IP Address Configuration : DHCP
```

```
IP Address : 30.30.30.26
IP Netmask : 255.255.255.0
Gateway IP Address : 30.30.30.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Capwap Active Window Size : 1
Telnet State : Disabled
CPU Type : ARMv8 Processor rev 4 (v8l)
Memory Type : DDR3
Memory Size : 1752064 KB
SSH State : Enabled
Serial Console State : Enabled
```

Information About AP Audit Configuration

The AP Audit Configuration feature helps to detect wireless service synchronization issues between the controller and an AP. In Cisco IOS XE Amsterdam, Release 17.3.1, two methods are implemented to support AP audit configuration.

- Config Checker: This functionality helps in auditing the application of wireless policies during the AP join phase. Any discrepancies at this stage is reported on the controller. This is a built-in functionality and you cannot disable the same. When you try to configure any of the AP attributes such as name, IP address, controller information, tag, mode, radio mode, and radio admin state, the AP parses the CAPWAP payload configuration from the controller and reports errors detected back to the controller with proper code. If a discrepancy is detected, the controller flags errors using the syslog.
- Config Audit: This functionality helps to perform periodic comparison of operational states between an AP and the controller after the AP join phase and while the corresponding AP is still connected. Discrepancies, if any, are reported immediately on the controller. The consolidated report is available at the controller anytime. This functionality is disabled by default. The periodic auditing interval is a configurable parameter.

  Use the **ap audit-report** command to enable and configure audit report parameters. When triggered, AP sends configurations from the database to the controller, and the controller compares the configurations against the current configuration. If a discrepancy is detected, the controller flags the error using the syslog.

Restrictions for AP Audit Configuration

- Config checker alerts are available only through the syslog.
- IOS AP is not supported.
- The audit reports are not synchronized from the active to the standby controller. After SSO, they are not readily available until the next reporting interval of the already-connected APs.
- The audit reports are not available when an AP is in standalone mode.
- This feature is supported only on APs in FlexConnect mode.

Configure AP Audit Parameters (CLI)

The AP Audit Configuration feature helps you compare the operational states between an AP and the controller. The AP sends state view details to the controller, and the controller compares it with what it perceives as the AP state. This feature is disabled by default.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap audit-report enable** **Example:** `Device(config)# ap audit-report enable`	Enables audit reporting.
Step 3	**ap audit-report interval** *interval* **Example:** `Device(config)# ap audit-report interval 1300`	Configures AP audit reporting interval. The default value for interval is 1440 minutes. The valid range is from 10 to 43200.

Verifying AP Audit Report Summary

To verify the AP audit report summary, use the **ap audit-report summary** command:

```
Device# show ap audit-report summary
WTP Mac                    Radio                   Wlan                IPv4 Acl
IPv6 Acl       Last Report Time
-------------------------------------------------------------------------------------
1880.90fd.6b40   OUT_OF_SYNC    OUT_OF_SYNC    IN_SYNC        IN_SYNC        01/01/1970
05:30:00 IST
```

Verifying AP Audit Report Detail

To verify an AP audit report's details, use the **show ap name ap-name audit-report detail** command:

```
Device# show ap name Cisco-AP audit-report detail
Cisco AP Name   : Cisco-AP
================================================
 IPV4 ACL Audit Report Status     : IN_SYNC

IPV6 ACL Audit Report Status     : IN_SYNC

Radio Audit Report Status        : IN_SYNC

WLAN Audit Report Status         :
Slot-id  Wlan-id  Vlan           State          SSID           Auth-Type      Other-Flag
-------------------------------------------------------------------------------------
```

```
0        4        IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC
1        4        IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC

bh-csr1#show ap audit-report summary
WTP-Mac          Radio          Wlan           IPv4-Acl       IPv6-Acl       Last-Report-Time
-------------------------------------------------------------------------------------------------
4001.7aca.5140   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:17:39 IST
4001.7aca.5a60   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:18:25 IST
7070.8b23.a1a0   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:18:29 IST
a0f8.49dc.9460   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:16:43 IST
a0f8.49dc.96e0   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:17:55 IST
```

2.4-GHz Radio Support

Configuring 2.4-GHz Radio Support for the Specified Slot Number

Before you begin

Note The term *802.11b radio* or *2.4-GHz radio* will be used interchangeably.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 24ghz slot 0 SI** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI`	Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point. For more information, *Spectrum Intelligence* section in this guide. Here, **0** refers to the Slot ID.
Step 3	**ap name** *ap-name* **dot11 24ghz slot 0 antenna** {**ext-ant-gain** *antenna_gain_value* | **selection** [**internal** | **external**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 antenna selection internal`	Configures 802.11b antenna hosted on slot 0 for a specific access point. • **ext-ant-gain**: Configures the 802.11b external antenna gain. *antenna_gain_value*- Refers to the external antenna gain value in multiples of .5 dBi units. The valid range is from 0 to 4294967295.

	Command or Action	Purpose
		• **selection**: Configures the 802.11b antenna selection (internal or external). **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model. • Cisco Catalyst 9120E and 9130E APs support self-identifying antennas (SIA). Cisco Catalyst 9115E APs do not support SIA antennas. Although Cisco Catalyst 9115E APs work with SIA antennas, the APs do not auto-detect SIA antennas nor add the correct external gain.
Step 4	**ap name** *ap-name* **dot11 24ghz slot 0 beamforming** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming`	Configures beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point.
Step 5	**ap name** *ap-name* **dot11 24ghz slot 0 channel** {*channel_number* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto`	Configures advanced 802.11 channel assignment parameters for the 2.4-GHz radio hosted on slot 0 for a specific access point.
Step 6	**ap name** *ap-name* **dot11 24ghz slot 0 cleanair** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair`	Enables CleanAir for 802.11b radio hosted on slot 0 for a specific access point.

	Command or Action	Purpose
Step 7	**ap name** *ap-name* **dot11 24ghz slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A`	Configures 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point. Here, **A**: Is the antenna port A. **B**: Is the antenna port B. **C**: Is the antenna port C. **D**: Is the antenna port D.
Step 8	**ap name** *ap-name* **dot11 24ghz slot 0 shutdown** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown`	Disables 802.11b radio hosted on slot 0 for a specific access point.
Step 9	**ap name** *ap-name* **dot11 24ghz slot 0 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 txpower auto`	Configures transmit power level for 802.11b radio hosted on slot 0 for a specific access point. • *tx_power_level*: Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**: Enables auto-RF.

5-GHz Radio Support

Configuring 5-GHz Radio Support for the Specified Slot Number

Before you begin

Note The term *802.11a radio* or *5-GHz radio* will be used interchangeably in this document.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**ap name** *ap-name* **dot11 5ghz slot 1 SI** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 SI`	Enables Spectrum Intelligence (SI) for the dedicated 5-GHz radio hosted on slot 1 for a specific access point. Here, **1** refers to the Slot ID.
Step 3	**ap name** *ap-name* **dot11 5ghz slot 1 antenna ext-ant-gain** *antenna_gain_value* **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna ext-ant-gain`	Configures external antenna gain for 802.11a radios for a specific access point hosted on slot 1. *antenna_gain_value*—Refers to the external antenna gain value in multiples of .5 dBi units. The valid range is from 0 to 4294967295. **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model. • Cisco Catalyst 9120E and 9130E APs support self-identifying antennas (SIA). Cisco Catalyst 9115E APs do not support SIA antennas. Although Cisco Catalyst 9115E APs work with SIA antennas, the APs do not auto-detect SIA antennas nor add the correct external gain.
Step 4	**ap name** *ap-name* **dot11 5ghz slot 1 antenna mode** [**omni** | **sectorA** | **sectorB**] **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna mode sectorA`	Configures the antenna mode for 802.11a radios for a specific access point hosted on slot 1.

	Command or Action	Purpose
Step 5	**ap name** *ap-name* **dot11 5ghz slot 1 antenna selection** [**internal** | **external**] **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna selection internal`	Configures the antenna selection for 802.11a radios for a specific access point hosted on slot 1.
Step 6	**ap name** *ap-name* **dot11 5ghz slot 1 beamforming** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 beamforming`	Configures beamforming for the 5-GHz radio hosted on slot 1 for a specific access point.
Step 7	**ap name** *ap-name* **dot11 5ghz slot 1 channel** {*channel_number* | **auto** | **width** [**20** | **40** | **80** | **160**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 channel auto`	Configures advanced 802.11 channel assignment parameters for the 5-GHz radio hosted on slot 1 for a specific access point. Here, *channel_number*- Refers to the channel number. The valid range is from 1 to 173.
Step 8	**ap name** *ap-name* **dot11 5ghz slot 1 cleanair** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 cleanair`	Enables CleanAir for 802.11a radio hosted on slot 1 for a given or specific access point.
Step 9	**ap name** *ap-name* **dot11 5ghz slot 1 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 dot11n antenna A`	Configures 802.11n for 5-GHz radio hosted on slot 1 for a specific access point. Here, **A**- Is the antenna port A. **B**- Is the antenna port B. **C**- Is the antenna port C. **D**- Is the antenna port D.
Step 10	**ap name** *ap-name* **dot11 5ghz slot 1 rrm channel** *channel* **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 rrm channel 2`	Is another way of changing the channel hosted on slot 1 for a specific access point. Here, *channel*- Refers to the new channel created using 802.11h channel announcement. The valid range is from 1 to 173, provided 173 is a valid channel in the country where the access point is deployed.
Step 11	**ap name** *ap-name* **dot11 5ghz slot 1 shutdown** **Example:**	Disables 802.11a radio hosted on slot 1 for a specific access point.

	Command or Action	Purpose
	`Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 shutdown`	
Step 12	**ap name** *ap-name* **dot11 5ghz slot 1 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 txpower auto`	Configures 802.11a radio hosted on slot 1 for a specific access point. • *tx_power_level*- Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**- Enables auto-RF.

6-GHz Radio Support

Configuring 6-GHz Radio Support for the Specified Slot Number

Before you begin

Static channel must be set before changing the channel width.

As there are no external antenna APs, as by regulatory requirements, antennas have to be captive (internal always) for 6-GHz.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 6ghz slot 3 antenna port** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 antenna port A`	Configures the antenna port for 802.11 6-Ghz radios for a specific access point. Here, **A**: Is the antenna port A. **B**: Is the antenna port B. **C**: Is the antenna port C. **D**: Is the antenna port D.
Step 3	**ap name** *ap-name* **dot11 6ghz slot 3 antenna selection** [**internal** | **external**] **Example:**	Configures the antenna selection, either internal or external, for 802.11 6-Ghz radios for a specific access point.

	Command or Action	Purpose
	`Device# ap name Cisco-AP dot11 6ghz slot 1 antenna selection internal`	**Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model. • Cisco Catalyst 9120E and 9130E APs support self-identifying antennas (SIA). Cisco Catalyst 9115E APs do not support SIA antennas. Although Cisco Catalyst 9115E APs work with SIA antennas, the APs do not auto-detect SIA antennas nor add the correct external gain.
Step 4	**ap name** *ap-name* **dot11 6ghz slot 3 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 channel auto`	Configures advanced 802.11 channel assignment parameters for the 6-GHz radio hosted on slot 3 for a specific access point. Here, *channel_number*: Refers to the channel number. The valid range is from 1 to 233.
Step 5	**ap name** *ap-name* **dot11 6ghz slot 3 dot11ax bss-color** {*bss-color-number* | **auto**} **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 dot11ax bss-color auto`	Enables basic service set (BSS) color for 802.11 6-Ghz radio for a given or specific access point. Here, *bss-color-number*: Refers to the BSS color number. The valid range is from 1 to 63.
Step 6	**ap name** *ap-name* **dot11 6ghz slot 3 radio role** {**auto** | **manual** {**client-serving** | **monitor** | **sniffer**}} **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 radio role auto`	Configures the 802.11 6-Ghz radio role, which is either **auto** or **manual**.

	Command or Action	Purpose
Step 7	**ap name** *ap-name* **dot11 6ghz slot 3 rrm channel** *channel* **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 rrm channel 1`	Configures a new channel using 802.11h channel announcement. Here, *channel*: Refers to the new channel created using 802.11h channel announcement. The valid range is from 1 to 233.
Step 8	**ap name** *ap-name* **dot11 6ghz slot 3 shutdown** **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 shutdown`	Disables the 802.11 6-Ghz radio on the Cisco AP.
Step 9	**ap name** *ap-name* **dot11 6ghz slot 3 txpower** {*tx_power_level* | **auto**} **Example:** `# ap name AP-SIDD-A06 dot11 5ghz slot 1 txpower auto`	Configures 802.11 6-Ghz Tx power level. • *tx_power_level*: Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**: Enables auto-RF.

Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in Cisco 2800, 3800, 4800, and the 9120 series AP models offer the ability to serve 2.4–GHz or 5–GHz bands or passively monitor both the bands on the same AP. These APs can be configured to serve clients in 2.4–GHz and 5–GHz bands, or serially scan both 2.4–GHz and 5–GHz bands on the flexible radio while the main 5–GHz radio serves clients.

Cisco Catalyst Wireless 9166 AP (CW9166) now has XOR function for a dual 5-GHz 4x4 or 5-GHz 4x4 and 6-GHz 4x4 radios. These radios can also be configured as client serving, monitor or as a sniffer interface like the earlier XOR radios.

Note For all countries that do not support 6-GHz spectrum for use of Wi-Fi, when the Cisco Catalyst Wireless 9166I AP operates as dual 5-GHz, the 5-GHz channels will be locked on both the radios even if slot 2 is disabled or set up for monitoring.

Cisco APs models up and through the Cisco 9120 APs are designed to support dual 5–GHz band operations with the *i* model supporting a dedicated Macro/Micro architecture and the *e* and *p* models supporting Macro/Macro. The Cisco 9130AXI APs and the Cisco 9136 APs support dual 5-GHz operations as Micro/Messo cell, and the CW9166I supports as Macro/Macro.

When a radio moves between bands (from 2.4-GHz to 5-GHz and vice versa), clients need to be steered to get an optimal distribution across radios. When an AP has two radios in the 5–GHz band, client steering algorithms contained in the Flexible Radio Assignment (FRA) algorithm are used to steer a client between the same band co-resident radios.

The XOR radio support can be steered manually or automatically:

- Manual steering of a band on a radio—The band on the XOR radio can only be changed manually.

- Automatic client and band steering on the radios is managed by the FRA feature that monitors and changes the band configurations as per site requirements.

Note RF measurement will not run when a static channel is configured on slot 1. Due to this, the dual band radio slot 0 will move only with 5–GHz radio and not to the monitor mode.

When slot 1 radio is disabled, RF measurement will not run, and the dual band radio slot 0 will be only on 2.4–GHz radio.

Note Only one of the 5-GHz radios can operate in the UNII band (100 - 144), due to an AP limitation to keep the power budget within the regulatory limit.

Configuring Default XOR Radio Support

Before you begin

Note The default radio points to the XOR radio hosted on slot 0.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* **Example:** `Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	Configures the 802.11 dual-band antenna on a specific Cisco access point. *antenna_gain_value*: The valid range is from 0 to 40.
Step 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** **Example:** `Device# ap name ap-name dot11 dual-band shutdown`	Shuts down the default dual-band radio on a specific Cisco access point. Use the **no** form of the command to enable the radio.
Step 4	**ap name** *ap-name* **dot11 dual-band role manual client-serving** **Example:**	Switches to client–serving mode on the Cisco access point.

	Command or Action	Purpose
	`Device# ap name ap-name dot11 dual-band role manual client-serving`	
Step 5	**ap name** *ap-name* **dot11 dual-band band 24ghz** **Example:** `Device# ap name ap-name dot11 dual-band band 24ghz`	Switches to 2.4-GHz radio band.
Step 6	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} **Example:** `Device# ap name ap-name dot11 dual-band txpower 2`	Configures the transmit power for the radio on a specific Cisco access point. **Note** When an FRA-capable radio (slot 0 on 9120 AP[for instance]) is set to Auto, you cannot configure static channel and Txpower on this radio. If you want to configure static channel and Txpower on this radio, you will need to change the radio role to Manual Client-Serving mode. This note is not applicable for Cisco Catalyst Wireless 9166 AP (CW9166).
Step 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* **Example:** `Device# ap name ap-name dot11 dual-band channel 2`	Enters the channel for the dual band. *channel-number*—The valid range is from 1 to 173.
Step 8	**ap name** *ap-name* **dot11 dual-band channel auto** **Example:** `Device# ap name ap-name dot11 dual-band channel auto`	Enables the auto channel assignment for the dual-band.
Step 9	**ap name** *ap-name* **dot11 dual-band channel width** {**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} **Example:** `Device# ap name ap-name dot11 dual-band channel width 20 MHz`	Chooses the channel width for the dual band.
Step 10	**ap name** *ap-name* **dot11 dual-band cleanair** **Example:**	Enables the Cisco CleanAir feature on the dual-band radio.

	Command or Action	Purpose
	`Device# ap name ap-name dot11 dual-band cleanair`	

Step 11	**ap name** *ap-name* **dot11 dual-band cleanair band**{**24 GHz | 5 GMHz**}
	Example:
	`Device# ap name ap-name dot11 dual-band cleanair band 5 GHz`
	`Device# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz`
		Selects a band for the Cisco CleanAir feature.
		Use the **no** form of this command to disable the Cisco CleanAir feature.

Step 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A | B | C | D**} **Example:** `Device# ap name ap-name dot11 dual-band dot11n antenna A`	Configures the 802.11n dual-band parameters for a specific access point.
Step 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** **Example:** `Device# show ap name ap-name auto-rf dot11 dual-band`	Displays the auto-RF information for the Cisco access point.
Step 14	**show ap name** *ap-name* **wlan dot11 dual-band** **Example:** `Device# show ap name ap-name wlan dot11 dual-band`	Displays the list of BSSIDs for the Cisco access point.

Configuring XOR Radio Support for the Specified Slot Number (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** section, select the AP for which you want to configure dual-band radios.

The AP name, MAC address, CleanAir capability and slot information for the AP are displayed. If the Hyperlocation method is HALO, the antenna PID and antenna design information are also displayed.

Step 3 Click **Configure**.

Step 4 In the **General** tab, set the **Admin Status** as required.

Step 5 Set the **CleanAir Admin Status** field to Enable or Disable.

Step 6 Click **Update & Apply to Device**.

Configuring XOR Radio Support for the Specified Slot Number

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point. *external_antenna_gain_value* - Is the external antenna gain value in multiples of .5 dBi unit. The valid range is from 0 to 40. **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model.
Step 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	Configures current band for the XOR radio hosted on slot 0 for a specific access point.
Step 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	Configures dual-band channel for the XOR radio hosted on slot 0 for a specific access point. *channel_number*- The valid range is from 1 to 165.

	Command or Action	Purpose
Step 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	Enables CleanAir features for dual-band radios hosted on slot 0 for a specific access point.
Step 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	Configures 802.11n dual-band parameters hosted on slot 0 for a specific access point. Here, **A**- Enables antenna port A. **B**- Enables antenna port B. **C**- Enables antenna port C. **D**- Enables antenna port D.
Step 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	Configures dual-band role for the XOR radio hosted on slot 0 for a specific access point. The following are the dual-band roles: • **auto**- Refers to the automatic radio role selection. • **manual**- Refers to the manual radio role selection.

Step 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown**
	Example:
	`Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown`
	`Device# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`
		Disables dual-band radio hosted on slot 0 for a specific access point.
		Use the **no** form of this command to enable the dual-band radio.

Step 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	Configures dual-band transmit power for XOR radio hosted on slot 0 for a specific access point. • *tx_power_level*- Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**- Enables auto-RF.

Receiver Only Dual-Band Radio Support

Information About Receiver Only Dual-Band Radio Support

This feature configures the dual-band Rx-only radio features for an access point with dual-band radios.

This dual-band Rx-only radio is dedicated for Analytics, Hyperlocation, Wireless Security Monitoring, and BLE AoA*.

This radio will always continue to serve in monitor mode, therefore, you will not be able to make any channel and *tx-rx* configurations on the 3rd radio.

Configuring Receiver Only Dual-Band Parameters for Access Points

Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** settings, click the AP for which you want to configure the dual-band radios.

Step 3 In the **General** tab, enable the **CleanAir** toggle button.

Step 4 Click **Update & Apply to Device**.

Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.

Step 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 cleanair band** {**24Ghz** | **5Ghz**}
	Example:
	`Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 cleanair band 24Ghz`
	`Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 cleanair band 24Ghz`
		Enables CleanAir with receiver only (Rx-only) dual-band radio on a specific access point.
		Here, 2 refers to the slot ID.
		Use the **no** form of this command to disable CleanAir.

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** settings, click the AP for which you want to configure the dual-band radios.

Step 3 In the **General** tab, disable the **CleanAir Status** toggle button.

Step 4 Click **Update & Apply to Device**.

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.

Step 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 shutdown**
	Example:
	`Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 shutdown`
	`Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 shutdown`
		Disables receiver only dual-band radio on a specific Cisco access point.
		Here, 2 refers to the slot ID.
		Use the **no** form of this command to enable receiver only dual-band radio.

Configuring Client Steering (CLI)

Before you begin

Enable Cisco CleanAir on the corresponding dual-band radio.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**wireless macro-micro steering transition-threshold balancing-window** *number-of-clients(0-65535)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold balancing-window 10`	Configures the micro-macro client load–balancing window for a set number of clients.
Step 4	**wireless macro-micro steering transition-threshold client count** *number-of-clients(0-65535)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold client count 10`	Configures the macro-micro client parameters for a minimum client count for transition.
Step 5	**wireless macro-micro steering transition-threshold macro-to-micro** *RSSI-in-dBm(–128—0)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold macro-to-micro -100`	Configures the macro–to–micro transition RSSI.
Step 6	**wireless macro-micro steering transition-threshold micro-to-macro** *RSSI-in-dBm(–128—0)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold micro-to-macro -110`	Configures the micro–to–macro transition RSSI.
Step 7	**wireless macro-micro steering probe-suppression aggressiveness** *number-of-cycles(–128—0)* **Example:** `Device(config)# wireless macro-micro steering probe-suppression aggressiveness -110`	Configures the number of probe cycles to be suppressed.
Step 8	**wireless macro-micro steering probe-suppression hysteresis** *RSSI-in-dBm* **Example:** `Device(config)# wireless macro-micro steering probe-suppression hysteresis -5`	Configures the macro-to-micro probe in RSSI. The range is between –6 to –3.

	Command or Action	Purpose
Step 9	**wireless macro-micro steering probe-suppression probe-only** **Example:** `Device(config)# wireless macro-micro steering probe-suppression probe-only`	Enables probe suppression mode.
Step 10	**wireless macro-micro steering probe-suppression probe-auth** **Example:** `Device(config)# wireless macro-micro steering probe-suppression probe-auth`	Enables probe and single authentication suppression mode.
Step 11	**show wireless client steering** **Example:** `Device# show wireless client steering`	Displays the wireless client steering information.

Verifying Cisco Access Points with Dual-Band Radios

To verify the access points with dual-band radios, use the following command:

```
Device# show ap dot11 dual-band summary

AP Name Subband Radio      Mac   Status Channel Power Level Slot ID Mode
-------------------------------------------------------------------------------
4800   All 3890.a5e6.f360 Enabled (40)* *1/8     (22 dBm)      0   Sensor
4800   All 3890.a5e6.f360 Enabled N/A    N/A       2              Monitor
```

Information About OFDMA Support for 11ax Access Points

The Cisco Catalyst 9100 series access points are the next generation WiFi 802.11ax access point, which is ideal for high-density high-definition applications.

The IEEE 802.11ax protocol aims to improve user experience and network performance in high density deployments for both 2.4 GHz and 5 GHz. The 802.11ax APs supports transmission or reception to more than one client simultaneously using Orthogonal Frequency Division Multiplexing (OFDMA).

The IEEE 802.11ax supports uplink MU-MIMO and also adds OFDMA for multiple users in the uplink and downlink. All the users in IEEE 802.11ax OFDMA have the same time allocations and it ends at the same time. In MU-MIMO and OFDMA, multiple stations (STAs) either simultaneously transmit to a single STA or simultaneously receive from a single STA independent data streams over the same radio frequencies.

Supported Modes on 11ax Access Points

The following AP modes are supported:

- Local mode
- Flex-connect mode

- Bridge mode
- Flex+Mesh mode

Configuring 11AX (GUI)

You can configure 11ax for the frequencies, 5 GHz and 2.4 GHz.

Procedure

Step 1 Choose **Configuration > Radio Configurations > High Throughput**.

Step 2 Click the **5 GHz Band** tab.

a) Expand the **11ax** section.
b) Select the **Enable 11ax** and **Multiple Bssid** check boxes, if required.
c) Check either the **Select All** check box to configure all the data rates or select the desired options from the available data rates list.

Step 3 Click the **2.4 GHz Band** tab.

a) Expand the **11ax** section.
b) Select the **Enable 11ax** and **Multiple Bssid** check boxes, if required.
c) Check either the **Select All** check box to configure all the data rates or select the desired options from the available data rates list.

Configuring Channel Width

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca chan-width 160** **Example:** `Device(config)# ap dot11 5ghz rrm channel dca chan-width 160`	Configures channel width for 802.11 radios as 160. Use the **no** form of the command to disable the configuration. **Note** Cisco Catalyst 9115 and C9120 series APs do not support 80+80 channel width. Cisco Catalyst 9117 series APs do not support OFDMA in 160 channel width.

	Command or Action	Purpose
Step 3	**ap dot11** { **24ghz** | **5ghz** } **rf-profile** *profile-name* **Example:** `Device(config)# ap dot11 5ghz rf-profile ax-profile`	Configures an RF profile and enters RF profile configuration mode.
Step 4	**channel chan-width 160** **Example:** `Device(config-rf-profile)# channel chan-width 160`	Configures the RF profile DCA channel width.

Configuring 802.11ax Radio Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **High Throughput** > **5 GHz Band** > **11ax**.

Step 2 Check or uncheck the **Enable 11 n** check box.

Step 3 Check the check boxes for the desired MCS/(data rate) or to select all of them, check the **Select All** check box.

Step 4 Click **Apply**.

Step 5 Choose **Configuration** > **Radio Configurations** > **High Throughput** > **2.4 GHz Band** > **11ax**.

Step 6 Check or uncheck the **Enable 11 n** check box.

Step 7 Check the check boxes for the desired MCS/(data rate) or to select all of them, check the **Select All** check box.

Step 8 Click **Apply**.

Step 9 Choose **Configuration** > **Wireless** > **Access Points**.

Step 10 Click the Access Point.

Step 11 In the **Edit AP** dialog box, enable the **LED State** toggle button and choose the LED brightness level from the **LED Brightness Level** drop-down list.

Step 12 Click **Update and Apply to Device**.

Configuring 802.11ax Radio Parameters (CLI)

Follow the procedure given below to configure radio parameters:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap dot11** { **24ghz** | **5ghz** | **6ghz** } **dot11ax** **Example:** `Device(config)# ap dot11 6ghz dot11ax`	Configures 802.11 6GHz dot11ax parameters. Use the **no** form of the command to disable the configuration.
Step 3	**ap dot11** { **24ghz** | **5ghz** | **6ghz** } **dot11ax mcs tx index** *index* **spatial-stream** *spatial-stream-value* **Example:** `Device(config)# ap dot11 5ghz dot11ax mcs tx index 11 spatial-stream 8`	Enables the 11ax 2.4-Ghz, 5-Ghz, or 6-Ghz band modulation and coding scheme (MCS) transmission rates.
Step 4	**ap led-brightness** *brightness-level* **Example:** `Device(config)# ap led-brightness 6`	(Optional) Configures the led brightness level.

Setting up the 802.11ax Radio Parameters

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **led-brightness-level** *brightness-level* **Example:** `Device# ap name ax-ap led-brightness-level 6`	Configures the led brightness level.
Step 3	**ap name** *ap-name***dot11** { **24ghz** | **5ghz** } **dot11n antenna** *antenna-port* **Example:** `Device# ap name ap1 dot11 5ghz dot11n antenna A`	Configures the 802.11n - 5 GHz antenna selection. Use the **no** form of the command to disable the configuration.

	Command or Action	Purpose
Step 4	**ap name** *ap-name* **dot11** { **24ghz** | **5ghz** } **channel width** *channel-width* **Example:** `Device# ap name ap1 dot11 5ghz channel width 160`	Configures 802.11 channel width.
Step 5	**ap name** *ap-name* **dot11** { **24ghz** | **5ghz** } **secondary-80** *channel-num* **Example:** `Device# ap name ap1 dot11 5ghz secondary-80 12`	Configures the advanced 802.11 secondary 80Mhz channel assignment parameters.

Configuring OFDMA on a WLAN

Note For Cisco Catalyst 9115 and 9120 series APs, the configuration given below are per radio, and not per WLAN. This feature remains enabled on the controller, if it is enabled on any of the WLANs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wlan** *wlan1* **Example:** `Device(config)# wlan wlan1`	Enters the WLAN configuration mode.
Step 3	**dot11ax** *downlink-ofdma* **Example:** `Device(config-wlan)# dot11ax downlink-ofdma`	Enables the downlink connection that uses the OFDMA technology. Use the **no** form of the command to disable the configuration.
Step 4	**dot11ax** *uplink-ofdma* **Example:** `Device(config-wlan)# dot11ax uplink-ofdma`	Enables the uplink connection that uses the OFDMA technology .
Step 5	**dot11ax** *downlink-mumimo* **Example:**	Enables the downlink connection that uses the MUMIMO technology.

	Command or Action	Purpose
	`Device(config-wlan)# dot11ax downlink-mumimo`	
Step 6	**dot11ax** *uplink-mumimo* **Example:** `Device(config-wlan)# dot11ax uplink-mumimo`	Enables the uplink connection that uses the MUMIMO technology.
Step 7	**dot11ax** *twt-broadcast-support* **Example:** `Device (config-wlan)# dot11ax twt-broadcast-support`	Enables the TWT broadcast support operation.

Verifying Channel Width

To verify the channel width and other channel information, use the following **show** commands:

```
Device# show ap dot11 5ghz summary

AP Name             Mac Address       Slot    Admin State  Oper State  Channel    Width
 Txpwr
-------------------------------------------------------------------------------------------------
AP80e0.1d75.6954    80e0.1d7a.7620     1       Enabled      Up          (52)*      160
  1(*)

Device# show ap dot11 dual-band summary

AP Name         Subband    Radio Mac        Status     Channel    Power Level  Slot ID
   Mode
-------------------------------------------------------------------------------------------------
kartl28021mi    All        002a.1058.38a0    Enabled   (52)*      (1)*           1
   REAP

Device# show ap name <ap-name> channel

802.11b/g Current Channel                        : 11
Slot ID                                          : 0
Allowed Channel List                             : 1,2,3,4,5,6,7,8,9,10,11
802.11a Current Channel ..................... 52  (160 MHz)
Slot ID                                          : 1
Allowed Channel List                             :
36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,149,153,157,161,165

Device# show ap name <ap-name> config slot <slot-num>
.
.
.
Phy OFDM Parameters
             Configuration                               : Automatic
             Current Channel                             : 52
             Extension Channel                           : No Extension
             Channel Width                               : 160 MHz
            Allowed Channel List                         :
36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,149,153,157,161,165
             TI Threshold                                : 0
```

```
Device# show ap dot11 5ghz channel
.
.
.
  DCA Sensitivity Level                     : MEDIUM : 15 dB
  DCA 802.11n/ac Channel Width              : 160 MHz
  DCA Minimum Energy Limit                  : -95 dBm
.
.
.
Device# show ap rf-profile name <name> detail
.
.
.
Unused Channel List               : 165
DCA Bandwidth                     :  160 MHz
DCA Foreign AP Contribution       : Enabled
.
.
.
```

Verifying Client Details

To verify the client information, use the following **show** commands:

```
Device# show wireless client mac-address <mac-address> detail


Client MAC Address : a886.ddb2.05e9
Client IPv4 Address : 169.254.175.214
Client IPv6 Addresses : fe80::b510:a381:8099:4747
                        2009:300:300:57:4007:6abb:2c9a:61e2
Client Username: N/A
Voice Client Type   : Unknown
AP MAC Address : c025.5c55.e400
AP Name: APe4c7.22b2.948e
Device Type: N/A
Device Version: N/A
AP slot : 0
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id : 1
Wireless LAN Name: SSS_OPEN
BSSID : c025.5c55.e406
Connected For : 23 seconds
Protocol : 802.11ax - 5 GHz
Channel : 8
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 86400 sec (Remaining time: 86378 sec)

.
.
.
Device# show wireless client summary
```

```
Number of Local Clients: 1

MAC Address    AP Name                           WLAN  State             Protocol Method
  Role
-------------------------------------------------------------------------------------------------
a886.ddb2.05e9 APe4c7.22b2.948e                  1     Run               11ax(5) None
 Local

Device# show wireless stats client detail


Total Number of Clients : 1

Protocol Statistics

--------------------------------------------------------------------------------
Protocol            Client Count
 802.11b              : 0
 802.11g              : 0
 802.11a              : 0
 802.11n-2.4GHz       : 0
 802.11n-5 GHz        : 0
 802.11ac             : 0
 802.11ax-5 GHz       : 0
 802.11ax-2.4 GHz     : 0
 802.11ax-6 GHz       : 1
```

Verifying Radio Configuration

To verify the radio configuration information, use the following **show** commands:

```
Device# show ap dot11 5ghz network

802.11a Network                             : Enabled
.
.
.
802.11ax                                    : Enabled
  DynamicFrag                               : Enabled
  MultiBssid                                : Disabled
802.11ax MCS Settings:
  MCS  7, Spatial Streams = 1               : Disabled
  MCS  9, Spatial Streams = 1               : Disabled
  MCS 11, Spatial Streams = 1               : Disabled
  MCS  7, Spatial Streams = 2               : Supported
  MCS  9, Spatial Streams = 2               : Supported
  MCS 11, Spatial Streams = 2               : Supported
  MCS  7, Spatial Streams = 3               : Supported
  MCS  9, Spatial Streams = 3               : Disabled
  MCS 11, Spatial Streams = 3               : Disabled
  MCS  7, Spatial Streams = 4               : Supported
  MCS  9, Spatial Streams = 4               : Supported
  MCS 11, Spatial Streams = 4               : Supported
  MCS  7, Spatial Streams = 5               : Supported
  MCS  9, Spatial Streams = 5               : Supported
  MCS 11, Spatial Streams = 5               : Supported
  MCS  7, Spatial Streams = 6               : Supported
  MCS  9, Spatial Streams = 6               : Supported
  MCS 11, Spatial Streams = 6               : Supported
  MCS  7, Spatial Streams = 7               : Supported
  MCS  9, Spatial Streams = 7               : Supported
```

```
  MCS 11, Spatial Streams = 7             : Supported
  MCS  7, Spatial Streams = 8             : Supported
  MCS  9, Spatial Streams = 8             : Supported
  MCS 11, Spatial Streams = 8             : Supported
Beacon Interval                           : 100
.
.
.
Maximum Number of Clients per AP Radio    : 200
```

```
Device# show ap dot11 24ghz network

802.11b Network                           : Enabled
.
.
.
802.11axSupport..................................... Enabled
      dynamicFrag.............................. Disabled
      multiBssid............................... Disabled
802.11ax                                  : Enabled
  DynamicFrag                             : Enabled
  MultiBssid                              : Enabled
802.11ax MCS Settings:
  MCS  7, Spatial Streams = 1             : Supported
  MCS  9, Spatial Streams = 1             : Supported
  MCS 11, Spatial Streams = 1             : Supported
  MCS  7, Spatial Streams = 2             : Supported
  MCS  9, Spatial Streams = 2             : Supported
  MCS 11, Spatial Streams = 2             : Supported
  MCS  7, Spatial Streams = 3             : Supported
  MCS  9, Spatial Streams = 3             : Supported
  MCS 11, Spatial Streams = 3             : Supported
  MCS  7, Spatial Streams = 4             : Disabled
  MCS  9, Spatial Streams = 4             : Disabled
  MCS 11, Spatial Streams = 4             : Disabled
Beacon Interval                           : 100
.
.
.
Maximum Number of Clients per AP Radio    : 200
```

```
Device# show ap dot11 6ghz network
802.11 6Ghz Network                       : Enabled
802.11ax                                  : Enabled
.
.
.
802.11ax MCS Settings:
  MCS  7, Spatial Streams = 1             : Supported
  MCS  9, Spatial Streams = 1             : Supported
  MCS 11, Spatial Streams = 1             : Supported
  MCS  7, Spatial Streams = 2             : Supported
  MCS  9, Spatial Streams = 2             : Supported
  MCS 11, Spatial Streams = 2             : Supported
  MCS  7, Spatial Streams = 3             : Supported
  MCS  9, Spatial Streams = 3             : Supported
  MCS 11, Spatial Streams = 3             : Supported
  MCS  7, Spatial Streams = 4             : Supported
  MCS  9, Spatial Streams = 4             : Supported
  MCS 11, Spatial Streams = 4             : Supported
Beacon Interval                           : 95
.
.
.
Maximum Number of Clients per AP Radio    : 200
```

```
WiFi to Cellular RSSI Threshold           : -85 dbm
Client Network Preference                 : default

#show wlan id 1
WLAN Profile Name     : wlanon66
================================================
Identifier                                : 1
Description                               :
Network Name (SSID)                       : wlanon66
Status                                    : Enabled
Broadcast SSID                            : Enabled
Advertise-Apname                          : Enabled
Universal AP Admin                        : Disabled
Max Associated Clients per WLAN           : 0
Max Associated Clients per AP per WLAN    : 0
Max Associated Clients per AP Radio per WLAN   : 200
OKC                                       : Enabled
Number of Active Clients                  : 0
CHD per WLAN                              : Enabled
WMM                                       : Allowed
WiFi Direct Policy                        : Disabled
.
.
.
Operational State of Radio Bands
    2.4ghz                                : UP
    5ghz                                  : UP
    6ghz                                  : DOWN (Required config: Disable WPA2 and
Enable WPA3 & dot11ax)
DTIM period for 802.11a radio             :
DTIM period for 802.11b radio             :
Local EAP Authentication                  : Disabled
Mac Filter Authorization list name        : Disabled
Mac Filter Override Authorization list name    : Disabled
Accounting list name                      :
802.1x authentication list name           : Disabled
802.1x authorization list name            : Disabled
Security
    802.11 Authentication                 : Open System
.
.
.
802.11ac MU-MIMO                          : Enabled
802.11ax parameters
    802.11ax Operation Status             : Enabled
    OFDMA Downlink                        : Enabled
    OFDMA Uplink                          : Enabled
    MU-MIMO Downlink                      : Enabled
    MU-MIMO Uplink                        : Enabled
    BSS Target Wake Up Time               : Enabled
    BSS Target Wake Up Time Broadcast Support  : Enabled
.
.
.
```

Note For 6-GHz radio, the 802.11ax parameters are taken from the multi BSSID profile tagged to the corresponding 6-GHz RF profile of the AP. So, the WLAN dot11ax parameters are overridden by multi BSSID profile parameters in the case of 6-GHz. There are no changes for 2.4 and 5-GHz band WLANs. They continue to use the WLAN parameters for 802.11ax.

```
Device# show ap led-brightness-level summary

AP Name                          LED Brightness level
------------------------------------------------------
AP00FC.BA01.CC00                 Not Supported
AP70DF.2FA2.72EE                 8
AP7069.5A74.6678                 2
APb838.6159.e184                 Not Supported
```

Information About Cisco Flexible Antenna Port

The presence of multiple antennas on the transmitters and the receivers of access points (APs), results in better performance and reliability of the APs. Multiple antennas improve reception through the selection of stronger signals or a combination of individual signals, at the receiver. You can configure the antenna ports to be used in the APs as either dual-band antennas or as single-band antennas to optimize radio coverage.

- Dual-band antenna mode: APs operate in both the 2.4-GHz and 5-GHz bandwidth with all the four antennas—A, B, C, and D. An example of a dual-band antenna mode AP is the Cisco Industrial Wireless 3702 AP.
- Single-band antenna mode: Among the APs, antennas A and B operate in the 2.4-GHz bandwidth, and the antennas C and D operate in the 5-GHz bandwidth. An example of a single-band antenna mode AP is the Cisco Catalyst Industrial Wireless 6300 AP.

Configuring a Cisco Flexible Antenna Port (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Access Points**.

Step 2 Click **AP Name**.

Step 3 Click the **Advanced** tab.

Step 4 From the **Antenna Mode** drop-down list, choose the antenna mode.

Step 5 Click **Apply & Update**.

Configuring a Cisco Flexible Antenna Port (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **antenna-band-mode** {**dual** | **single**} **Example:**	Configures antenna band mode as single or dual.

	Command or Action	Purpose
	Device# ap name *ap-name* antenna-brand-mode single	

Verifying Flexible Antenna Port Configuration

The following is a sample output of the **show ap name** *ap_name* **config general** command that shows the bands selected on a specific AP:

```
Device# show ap name APXXXX.31XX.83XX config general
Cisco AP Name   : APXXXX.31XX.83XX
================================================
Cisco AP Identifier                             : b4de.312e.00c0
Country Code                                    : Multiple Countries : US,IN
Regulatory Domain Allowed by Country   : 802.11bg:-A   802.11a:-ABDN

AP Submode                                      : Not Configured
Antenna Band Mode                               : Dual
```

The following is a sample output of the **show ap name** *ap_name* **config slot 0** command that shows the bands selected on a specific AP with dual-band mode enabled:

```
Device# show ap name APXXXX.31XX.83XX config slot 0 | sec 802.11n Antennas
    802.11n Antennas
      A                                         : ENABLED
      B                                         : ENABLED
      C                                         : ENABLED
      D                                         : ENABLED

    802.11n Antennas
      MIMO                                      : x
      Tx                                        : Unknown
      Rx                                        : Unknown
```

The following is a sample output of the **show ap name** *ap_name* **config slot 1** command that shows the bands selected on a specific AP with single-band mode enabled:

```
Device# show ap name APXXXX.31XX.83XX config slot 1 | sec 802.11n Antennas
    802.11n Antennas
      A                                         : DISABLED
      B                                         : DISABLED
      C                                         : ENABLED
      D                                         : ENABLED

    802.11n Antennas
      MIMO                                      : x
      Tx                                        : Unknown
      Rx                                        : Unknown
```

Feature History for Environmental Sensors in Access Points

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 37: Feature History for Environmental Sensors on Access Points

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	Environmental Sensors in Access Points	The Environmental Sensors in Access Points feature helps you collect real-time environmental data, such as, air quality, temperature, and humidity, from the environmental sensors that are embedded in the Cisco Catalyst 9136 Series Access Points.
Cisco IOS XE Cupertino 17.9.1	Environmental Sensors in Access Points	This feature is supported on Cisco Catalyst Wireless 9166I Series Access Points.

Information About Environmental Sensors in Access Points

You can collect real-time environmental data, such as, air quality, temperature, and humidity, from the environmental sensors that are embedded in the Cisco Catalyst 9136 Series Access Points, and make this data available to customers and partners through the Cisco Spaces solution. You can disable, enable, and configure the scan interval of the sensors from the Cisco Catalyst 9800 Series Wireless Controller CLIs.

Note From Cisco IOS XE Cupertino 17.8.1, this feature is supported on Cisco Catalyst 9136 Series APs.

In Cisco IOS XE Cupertino 17.9.1, air quality, temperature, and humidity are supported on Cisco Catalyst Wireless 9166I Series Access Points.

Currently, two sensors are added to Cisco Catalyst 9136 Series APs:

- Total volatile organic compounds (TVOC) air quality sensor
- Combined Temperature and Humidity sensor

Use Cases

The following are the use cases for the environmental sensors in APs:

- In the healthcare industry, environmental sensors help reduce wastage and spoilage of pharmaceuticals by maintaining a consistent environment.
- In the hospitality industry, environmental sensors help improve customer experience by monitoring the air quality of a room.
- In the retail industry, these sensors prevent spoilage of products.

Configuring Environmental Sensors in an AP Profile (CLI)

To configure the environmental sensor in the Cisco Catalyst 9800 Series Wireless Controllers under an AP profile, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP profile.
Step 3	**sensor environment air-quality** **Example:** `Device(config-ap-profile)# sensor environment air-quality`	Configures AP environmental air quality sensor. Enters AP sensor configuration mode.
Step 4	**no shutdown** **Example:** `Device(config-ap-sensor)# no shutdown`	Enables the AP air quality sensor configuration.
Step 5	**sensor environment temperature** **Example:** `Device(config-ap-profile)# sensor environment temperature`	Configures AP environmental temperature sensor. Enters AP sensor configuration mode.
Step 6	**no shutdown** **Example:** `Device(config-ap-sensor)# no shutdown`	Enables the AP temperature sensor configuration.
Step 7	**sampling** *data-sampling-interval* **Example:** `Device(config-ap-sensor)# sampling 200`	Configures data sampling interval, in seconds. The valid range is between 5 and 3600. The default value is 5. Use the **no** form of this command to set the data sampling interval to the default time of 5.
Step 8	**exit** **Example:** `Device(config-ap-sensor)# exit`	Exits the sub mode.

Configuring Environment Sensors in Privileged EXEC Mode (CLI)

To disable the sensor on an AP that might be sending invalid data (an AP near an air vent or near a coffee machine), you can disable the sensor by running the corresponding commands in the privileged EXEC mode of the Cisco Catalyst 9800 Series Wireless Controllers.

Note For a sensor to be operational in the **Up** state, both, the AP profile configuration state and the AP administrative state should be enabled. If any of the two is disabled, the sensor operational status will stay **Down**.

To disable and enable the admin state of the sensor, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter the password if prompted.
Step 2	**ap name** *ap-name* **sensor environment**{**air-quality** | **temperature**} **shutdown** **Example:** `Device# ap name CiscoAP sensor environment air-quality shutdown`	Disables the sensor admin state of the AP.
Step 3	**ap name** *ap-name* **no sensor environment**{**air-quality** | **temperature**} **shutdown** **Example:** `Device# ap name CiscoAP no sensor environment air-quality shutdown`	Enables the sensor admin state of the AP.

Verifying the AP Sensor Status

To verify the status of the AP sensors, run the following command:

```
Device# show ap sensor status
AP Name                         MAC-address          Sensor-type      Config-State
Admin-State      Oper-Status      Sampling-Interval
-------------------------------------------------------------------------------------
Cisco.1DBC                       xxxx.xxxx.xxx1       Air-quality      Disabled
Enabled          Down            5
Cisco.1DBC                       xxxx.xxxx.xxx2       Temperature      Disabled
Enabled          Down            5
Cisco.1E24                       xxxx.xxxx.xxx3       Air-quality      Disabled
Enabled          Down            5
Cisco.1E24                       xxxx.xxxx.xxx4       Temperature      Disabled
Enabled          Down            5
```

Information About CAPWAP LAG Support

Link aggregation (LAG) simplifies controller configuration because you no longer require to configure primary and secondary ports for each interface. If any of the controller ports fail, traffic is automatically migrated to

one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

The CAPWAP LAG support feature is applicable for access points that support multiple ethernet ports for CAPWAP.

The 11AC APs with dual ethernet ports require the CAPWAP AP LAG support for data channel.

Cisco Aironet 1850, 2800, and 3800 Series APs' second Ethernet port is used as a link aggregation port, by default. It is possible to use this LAG port as an RLAN port when LAG is disabled.

The following APs use LAG port as an RLAN port:

- 1852E
- 1852I
- 2802E
- 2802I
- 3802E
- 3802I
- 3802P
- 9136I

Restrictions for CAPWAP LAG Support

- APs must be specifically enabled for CAPWAP AP LAG support.
- CAPWAP data does not support IPv6.
- Data DTLS must not be enabled when LAG is enabled.
- APs behind NAT and PAT are not supported.

Enabling CAPWAP LAG Support on Controller (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Wireless Global**.

Step 2 Check the **AP LAG Mode** check box.

Step 3 Click **Apply**.

Enabling CAPWAP LAG Support on Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lag support** **Example:** `Device(config)# ap lag support`	Enables CAPWAP LAG support on the controller. **Note** After executing this command, you get to view the following warning statement: *Changing the lag support will cause all the APs to disconnect.* Thus, all APs with LAG capability reboots and joins the enabled CAPWAP LAG.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling CAPWAP LAG Globally on Controller

If the CAPWAP LAG is enabled globally on the controller, the following occurs:

- AP joins the controller.
- AP exchanges its CAPWAP support.
- LAG mode starts, if LAG is enabled on AP.

Disabling CAPWAP LAG Globally on Controller

If the CAPWAP LAG is disabled globally on the controller, the following occurs:

- AP joins the controller.
- AP exchanges its CAPWAP support.
- AP LAG config is sent to AP, if LAG is already enabled on AP.
- AP reboots.

- AP joins back with the disabled LAG.

Enabling CAPWAP LAG for an AP Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click **Add**.

Step 3 Under the **General** tab, enter the **Name** of the AP Profile and check the **LAG Mode** check box to set the CAPWAP LAG for the AP profile.

Step 4 Click **Apply to Device**.

Enabling CAPWAP LAG for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**lag** **Example:** `Device(config-ap-profile)# lag`	Enables CAPWAP LAG for an AP profile.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Disabling CAPWAP LAG for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**no lag** **Example:** `Device(config-ap-profile)# no lag`	Disables CAPWAP LAG for an AP profile.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Disabling CAPWAP LAG Support on Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no ap lag support** **Example:** `Device(config)# no ap lag support`	Disables CAPWAP LAG support on the controller . **Note** All APs with LAG capability reboots and joins the disabled CAPWAP LAG.
Step 3	**end** **Example:**	Exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	

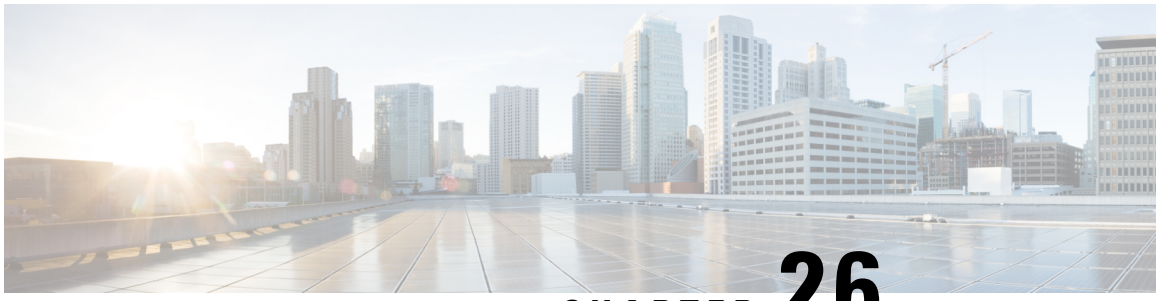
Verifying CAPWAP LAG Support Configurations

To verify the global LAG status for all Cisco APs, use the following command:

```
Device# show ap lag-mode
AP Lag-Mode Support Enabled
```

To verify the AP LAG configuration status, use the following command:

```
Device# show ap name <ap-name> config general
Cisco AP Identifier : 0008.3291.6360
Country Code : US
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-AB
AP Country Code : US - United States
::
AP Lag Configuration Status : Enabled/Disabled
Has AP negotiated lag based on AP capability and per AP config.
```



CHAPTER 26

Troubleshooting Lightweight Access Points

-
- Overview, on page 487
- Support Articles, on page 487
- Feedback Request, on page 488
- Disclaimer and Caution, on page 488

Overview

This chapter provides links to documents authored by Cisco subject matter experts (SMEs). They aim to help you resolve technical issues without requiring a support ticket. If these documents are unable to resolve your issue, we recommend visiting the applicable Cisco Community. There is a wealth of information and advice available from fellow Cisco customers who may have experienced this issue already and provided a solution. If you are not able to find a resolution on the Community, it may be best that you raise a support ticket at Cisco Support. In cases where a support ticket has to be raised, these documents provide guidance about the data that should be collected and added to the support ticket. Specify the support document you referred, and TAC can create an improvement request with the document owner.

Support Articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following are the support articles associated with this technology:

Document	Description
Troubleshoot Access Point Disassociation from Controller	This document provides use cases to understand the reason for the Control and Provisioning of Wireless Access Points (CAPWAP)/Lightweight Access Point Protocol (LWAPP) tunnel break between Access Points (APs) and the Wireless Controller.

Feedback Request

Your input helps. A key aspect to improving these support documents is customer feedback. Note that these documents are owned and maintained by multiple teams within Cisco. If you find an issue specific to the document (unclear, confusing, information missing, etc):

- Provide feedback using the **Feedback** button located at the right panel of the corresponding article. The document owner will be notified, and will either update the article, or flag it for removal.
- Include information regarding the section, area, or issue you had with the document and what could be improved. Provide as much detail as possible.

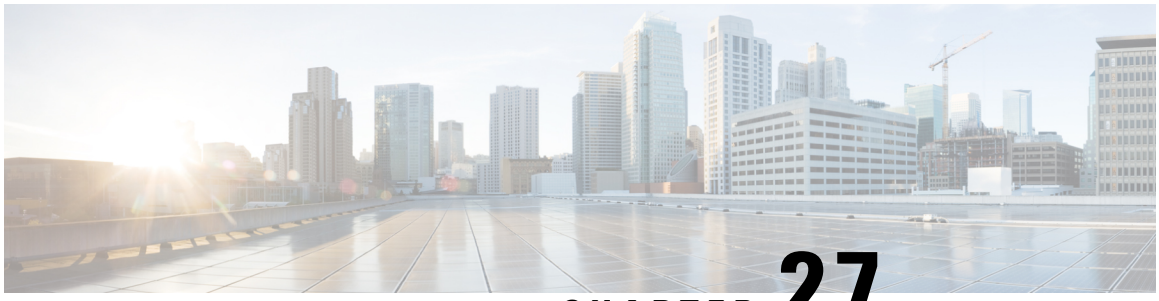
Disclaimer and Caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

PART IV

Radio Resource Management

- Radio Resource Management, on page 491
- Coverage Hole Detection, on page 527
- Optimized Roaming, on page 533
- Cisco Flexible Radio Assignment, on page 537
- XOR Radio Support, on page 547
- Cisco Receiver Start of Packet, on page 553
- Client Limit, on page 557
- IP Theft, on page 563
- Unscheduled Automatic Power Save Delivery, on page 569
- Target Wake Time, on page 571
- Enabling USB Port on Access Points, on page 577
- Dynamic Frequency Selection, on page 581
- Cisco Access Points with Tri-Radio, on page 587
- Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard, on page 593
- Antenna Disconnection Detection, on page 597
- Neighbor Discovery Protocol Mode on Access Points, on page 603
- 6-GHz Band Operations, on page 609



CHAPTER 27

Radio Resource Management

- Information About Radio Resource Management, on page 491
- Restrictions for Radio Resource Management, on page 501
- How to Configure RRM, on page 502
- Monitoring RRM Parameters and RF Group Status, on page 523
- Examples: RF Group Configuration, on page 524
- Information About ED-RRM, on page 524

Information About Radio Resource Management

The Radio Resource Management (RRM) software that is embedded in the device acts as a built-in Radio Frequency (RF) engineer to consistently provide real-time RF management of your wireless network. RRM enables devices to continually monitor their associated lightweight access points for the following information:

- Traffic load—The total bandwidth used for transmitting and receiving traffic. It enables wireless LAN managers to track and plan network growth ahead of client demand.
- Interference—The amount of traffic coming from other 802.11 sources.
- Noise—The amount of non-802.11 traffic that is interfering with the currently assigned channel.
- Coverage—The Received Signal Strength (RSSI) and signal-to-noise ratio (SNR) for all connected clients.
- Other —The number of nearby access points.

RRM performs these functions:

- Radio resource monitoring
- Power control transmission
- Dynamic channel assignment
- Coverage hole detection and correction
- RF grouping

Note RRM grouping does not occur when an AP operates in a static channel that is not in the DCA channel list. The Neighbor Discovery Protocol (NDP) is sent only on DCA channels; therefore, when a radio operates on a non-DCA channel, it does not receive NDP on the channel.

Radio Resource Monitoring

RRM automatically detects and configures new devices and lightweight access points as they are added to the network. It then automatically adjusts the associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can scan all the valid channels for the country of operation as well as for channels available in other locations. The access points in local mode go *offchannel* for a period not greater than 70 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

Note In the presence of voice traffic or other critical traffic (in the last 100 ms), access points can defer off-channel measurements. The access points also defer off-channel measurements based on the WLAN scan priority configurations.

Each access point spends only 0.2 percent of its time off channel. This activity is distributed across all the access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance.

Information About RF Groups

An RF group is a logical collection of controllers that coordinate to perform RRM in a globally optimized manner to perform network calculations on a per-radio basis. Separate RF groups exist for 2.4-GHz and 5-GHz networks. Clustering Cisco Catalyst 9800 Series Wireless Controller into a single RF group enables the RRM algorithms to scale beyond the capabilities of a single Cisco Catalyst 9800 Series Wireless Controller.

An RF group is created based on the following parameters:

- User-configured RF network name.
- Neighbor discovery performed at the radio level.
- Country list configured on the controller.

RF grouping runs between controllers .

Lightweight access points periodically send out neighbor messages over the air. Access points using the same RF group name validate messages from each other.

When access points on different controllers hear validated neighbor messages at a signal strength of –80 dBm or stronger, the controllers dynamically form an RF neighborhood in auto mode. In static mode, the leader is manually selected and the members are added to the RF Group.

Note RF groups and mobility groups are similar, in that, they both define clusters of controllers , but they are different in terms of their use. An RF group facilitates scalable, system-wide dynamic RF management, while a mobility group facilitates scalable, system-wide mobility and controller redundancy.

RF Group Leader

RF Group Leader can be configured in two ways as follows:

Note RF Group Leader is selected based on the controller with the greatest AP capacity (platform limit). If multiple controllers have the same capacity, the leader is selected based on the Group ID, which is a combination of the management IP address, AP capacity, random number, and so on. The one with the highest Group ID is selected as the leader.

- Auto Mode: In this mode, the members of an RF group elect an RF group leader to maintain a *primary* power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or RF group members experience major changes).
- Static Mode: In this mode, a user selects a controller as an RF group leader manually. In this mode, the leader and the members are manually configured and fixed. If the members are unable to join the RF group, the reason is indicated. The leader tries to establish a connection with a member every minute if the member has not joined in the previous attempt.

The RF group leader analyzes real-time radio data collected by the system, calculates the power and channel assignments, and sends them to each of the controllers in the RF group. The RRM algorithms ensure system-wide stability, and restrain channel and power scheme changes to the appropriate local RF neighborhoods.

Note When a controller becomes both leader and member for a specific radio, you get to view the IPv4 and IPv6 address as part of the group leader.

When a Controller A becomes a member and Controller B becomes a leader, the Controller A displays either IPv4 or IPv6 address of Controller B using the address it is connected.

So, if both leader and member are not the same, you get to view only one IPv4 or IPv6 address as a group leader in the member.

If Dynamic Channel Assignment (DCA) needs to use the worst-performing radio as the single criterion for adopting a new channel plan, it can result in pinning or cascading problems.

The main cause of both pinning and cascading is that any potential channel plan changes are controlled by the RF circumstances of the worst-performing radio. The DCA algorithm does not do this; instead, it does the following:

- Multiple local searches: The DCA search algorithm performs multiple local searches initiated by different radios in the same DCA run rather than performing a single global search that is driven by a single radio.

This change addresses both pinning and cascading, while maintaining the desired flexibility and adaptability of DCA and without jeopardizing stability.

- Multiple Channel Plan Change Initiators (CPCIs): Previously, the single worst radio was the sole initiator of a channel plan change. Now each radio in an RF group is evaluated and prioritized as a potential initiator. Intelligent randomization of the resulting list ensures that every radio is eventually evaluated, which eliminates the potential for pinning.
- Limiting the propagation of channel plan changes (Localization): For each CPCI radio, the DCA algorithm performs a local search for a better channel plan, but only the CPCI radio itself and its one-hop neighboring access points are actually allowed to change their current transmit channels. The impact of an access point triggering a channel plan change is felt only to within two RF hops from that access point, and the actual channel plan changes are confined to within a one-hop RF neighborhood. Because this limitation applies across all CPCI radios, cascading cannot occur.
- Non-RSSI-based cumulative cost metric: A cumulative cost metric measures how well an entire region, neighborhood, or network performs with respect to a given channel plan. The individual cost metrics of all the access points in that area are considered in order to provide an overall understanding of the channel plan's quality. These metrics ensure that the improvement or deterioration of each single radio is factored into any channel plan change. The objective is to prevent channel plan changes in which a single radio improves, but at the expense of multiple other radios experiencing a considerable performance decline.

The RRM algorithms run at a specified updated interval, which is 600 seconds by default. Between update intervals, the RF group leader sends keepalive messages to each of the RF group members and collects real-time RF data.

Note Several monitoring intervals are also available. See the Configuring RRM section for details.

RF Grouping Failure Reason Codes

RF Grouping failure reason codes and their explanations are listed below:

Table 38: RF Grouping Failure Reason Codes

Reason Code	Description
1	Maximum number (20) of controllers are already present in the group.
2	If the following conditions are met: • The request is from a similar powered controller and, • Controller is the leader for the other band, OR • Requestor group is larger.
3	Group ID do not match.
4	Request does not include source type.

Reason Code	Description
5	Group spilt message to all member while group is being reformed.
6	Auto leader is joining a static leader, during the process deletes all the members.
9	Grouping mode is turned off.
11	Country code does not match.
12	Controller is up in hierarchy compared to sender of join command (static mode). Requestor is up in hierarchy (auto mode).
13	Controller is configured as static leader and receives join request from another static leader.
14	Controller is already a member of static group and receives a join request from another static leader.
15	Controller is a static leader and receives join request from non-static member.
16	Join request is not intended to the controller. Controller name and IP do not match.
18	RF domain do not match.
19	Controller received a Hello packet at incorrect state.
20	Controller has already joined Auto leader, now gets a join request from static leader.
21	Group mode change. Domain name change from CLI. Static member is removed from CLI.
22	Max switch size (350) is reached

Additional Reference

Radio Resource Management White Paper: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_011.html

RF Group Name

A controller is configured in an RF group name, which is sent to all the access points joined to the controller and used by the access points as the shared secret for generating the hashed MIC in the neighbor messages. To create an RF group, you configure all of the controllers to be included in the group with the same RF group name.

If there is any possibility that an access point joined to a controller might hear RF transmissions from an access point on a different controller , you should configure the controller with the same RF group name. If

RF transmissions between access points can be heard, then system-wide RRM is recommended to avoid 802.11 interference and contention as much as possible.

Rogue Access Point Detection in RF Groups

After you have created an RF group of controller , you need to configure the access points connected to the controller to detect rogue access points. The access points will then select the beacon or probe-response frames in neighboring access point messages to see if they contain an authentication information element (IE) that matches that of the RF group. If the selection is successful, the frames are authenticated. Otherwise, the authorized access point reports the neighboring access point as a rogue, records its BSSID in a rogue table, and sends the table to the controller .

Secure RF Groups

Secure RF groups enable to encrypt and secure RF grouping and RRM message exchanges over DTLS tunnel. During the DTLS handshake controllers authenticate each other with wireless management trust-point certificate.

Note If a controller has to be part of secure RF-group, that controller must be part of the same mobility group.

Transmit Power Control

The device dynamically controls access point transmit power based on the real-time wireless LAN conditions.

The Transmit Power Control (TPC) algorithm increases and decreases an access point’s power in response to changes in the RF environment. In most instances, TPC seeks to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage, for example, if an access point fails or becomes disabled, TPC can also increase power on the surrounding access points. This feature is different from coverage hole detection, which is primarily concerned with clients. TPC provides enough RF power to achieve the required coverage levels while avoiding channel interference between access points. We recommend that you select TPCv1; TPCv2 option is deprecated. With TPCv1, you can select the channel aware mode; we recommend that you select this option for 5 GHz, and leave it unchecked for 2.4 GHz.

Overriding the TPC Algorithm with Minimum and Maximum Transmit Power Settings

The TPC algorithm balances RF power in many diverse RF environments. However, it is possible that automatic power control will not be able to resolve some scenarios in which an adequate RF design was not possible to implement due to architectural restrictions or site restrictions, for example, when all the access points must be mounted in a central hallway, placing the access points close together, but requiring coverage to the edge of the building.

In these scenarios, you can configure maximum and minimum transmit power limits to override TPC recommendations. The maximum and minimum TPC power settings apply to all the access points through RF profiles in a RF network.

To set the Maximum Power Level Assignment and Minimum Power Level Assignment, enter the maximum and minimum transmit power used by RRM in the fields in the **Tx Power Control** window. The range for these parameters is -10 to 30 dBm. The minimum value cannot be greater than the maximum value; the maximum value cannot be less than the minimum value.

If you configure a maximum transmit power, RRM does not allow any access point attached to the controller, to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, no access point will transmit above 11 dBm, unless the access point is configured manually.

Cisco APs support power level changes in 3 dB granularity. TPC Min and Max power settings allow for values in 1 dB increments. The resulting power level will be rounded to the nearest value supported in the allowed powers entry for the AP model and the current serving channel.

Each AP model has its own set of power levels localized for its regulatory country and region. Moreover, the power levels for the same AP model will vary based on the band and channel it is set to. For more information on Allowed Power Level vs. Actual power(in dBm), use the **show ap name <name> config slot <0|1|2|3>** command to view the specific number of power levels, the range of power levels allowed, and the current power level setting on the AP.

Dynamic Channel Assignment

Two adjacent access points on the same channel can cause either signal contention or signal collision. In a collision, data is not received by the access point. This functionality can become a problem, for example, when someone reading an e-mail in a café affects the performance of the access point in a neighboring business. Even though these are separate networks, someone sending traffic to the café on channel 1 can disrupt communication in an enterprise using the same channel. Devices can dynamically allocate access point channel assignments to avoid conflict and increase capacity and performance. Channels are *reused* to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a different access point far from the café, which is more effective than not using channel 1 altogether.

The device's Dynamic Channel Assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot simultaneously use 11 or 54 Mbps. By effectively reassigning channels, the device keeps adjacent channels that are separated.

Note We recommend that you use only nonoverlapping channels (1, 6, 11, and so on).

Note Channel change does not require you to shut down the radio.

The device examines a variety of real-time RF characteristics to efficiently handle channel assignments as follows:

- Access point received energy: The received signal strength measured between each access point and its nearby neighboring access points. Channels are optimized for the highest network capacity.
- Noise: Noise can limit signal quality at the client and access point. An increase in noise reduces the effective cell size and degrades user experience. By optimizing channels to avoid noise sources, the device can optimize coverage while maintaining system capacity. If a channel is unusable due to excessive noise, that channel can be avoided.
- 802.11 interference: Interference is any 802.11 traffic that is not a part of your wireless LAN, including rogue access points and neighboring wireless networks. Lightweight access points constantly scan all the channels looking for sources of interference. If the amount of 802.11 interference exceeds a predefined

configurable threshold (the default is 10 percent), the access point sends an alert to the device. Using the RRM algorithms, the device may then dynamically rearrange channel assignments to increase system performance in the presence of the interference. Such an adjustment could result in adjacent lightweight access points being on the same channel, but this setup is preferable to having the access points remain on a channel that is unusable due to an interfering foreign access point.

In addition, if other wireless networks are present, the device shifts the usage of channels to complement the other networks. For example, if one network is on channel 6, an adjacent wireless LAN is assigned to channel 1 or 11. This arrangement increases the capacity of the network by limiting the sharing of frequencies. If a channel has virtually no capacity remaining, the device may choose to avoid this channel. In huge deployments in which all nonoverlapping channels are occupied, the device does its best, but you must consider RF density when setting expectations.

- Load and utilization: When utilization monitoring is enabled, capacity calculations can consider that some access points are deployed in ways that carry more traffic than other access points, for example, a lobby versus an engineering area. The device can then assign channels to improve the access point that has performed the worst. The load is taken into account when changing the channel structure to minimize the impact on the clients that are currently in the wireless LAN. This metric keeps track of every access point's transmitted and received packet counts to determine how busy the access points are. New clients avoid an overloaded access point and associate to a new access point. This *Load and utilization* parameter is disabled by default.

The device combines this RF characteristic information with RRM algorithms to make system-wide decisions. Conflicting demands are resolved using soft-decision metrics that guarantee the best choice for minimizing network interference. The end result is optimal channel configuration in a three-dimensional space, where access points on the floor above and below play a major factor in an overall wireless LAN configuration.

Note DCA supports only 20-MHz channels in 2.4-GHz band.

Note In a Dynamic Frequency Selection (DFS) enabled AP environment, ensure that you enable the UNII2 channels option under the DCA channel to allow 100-MHz separation for the dual 5-GHz radios.

The RRM startup mode is invoked in the following conditions:

- In a single-device environment, the RRM startup mode is invoked after the device is upgraded and rebooted.
- In a multiple-device environment, the RRM startup mode is invoked after an RF Group leader is elected.
- You can trigger the RRM startup mode from the CLI.

The RRM startup mode runs for 100 minutes (10 iterations at 10-minute intervals). The duration of the RRM startup mode is independent of the DCA interval, sensitivity, and network size. The startup mode consists of 10 DCA runs with high sensitivity (making channel changes easy and sensitive to the environment) to converge to a steady-state channel plan. After the startup mode is finished, DCA continues to run at the specified interval and sensitivity.

Note DCA algorithm interval is set to 1 hour, but DCA algorithm always runs in default interval of 10 min, channel allocation occurs at 10-min intervals for the first 10 cycles, and channel changes occur as per the DCA algorithm every 10 min. After that the DCA algorithm goes back to the configured time interval. This is common for both DCA interval and anchor time because it follows the steady state.

Invoking channel update will not result in any immediate changes until the next DCA interval is triggered.

Note If Dynamic Channel Assignment (DCA)/Transmit Power Control (TPC) is turned off on the RF group member, and auto is set on RF group leader, the channel or TX power on a member gets changed as per the algorithm that is run on the RF group leader.

Dynamic Bandwidth Selection

While upgrading from 11n to 11ac, the Dynamic Bandwidth Selection (DBS) algorithm provides a smooth transition for various configurations.

The following pointers describe the functionalities of DBS:

- It applies an additional layer of bias on top of those applied to the core DCA, for channel assignment in order to maximize the network throughput by dynamically varying the channel width.
- It fine tunes the channel allocations by constantly monitoring the channel and Base Station Subsystem (BSS) statistics.
- It evaluates the transient parameters, such as 11n or 11ac client mix, load, and traffic flow types.
- It reacts to the fast-changing statistics by varying the BSS channel width or adapting to the unique and new channel orientations through 11ac for selection between 40 MHz and 80 MHz bandwidths.

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a “coverage hole” alert to the device. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The device discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the device mitigates the coverage hole by increasing the transmit power level for that specific access point. The device does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

Cisco AI Enhanced RRM

The AI Enhanced RRM is the next evolution of Cisco's award winning Radio Resource Management (RRM).

The RRM runs as a service in a Cisco Catalyst 9800 Series Wireless Controller. The Cisco RRM manages the RF Group (the components making up the RF Network) based on dynamic measurements between every AP and its neighbors stored in a local database for the entire RF Group. At runtime, the RRM draws the last 10 minutes of the collected data, and gently optimizes based on the current network conditions.

The AI Enhanced RRM integrates the power of Artificial Intelligence and Machine Learning to the reliable and trusted Cisco RRM product family algorithms in the Cloud.

Note The AI enhanced RRM is coordinated through the Cisco Catalyst Center (on-prem appliance) as a service. The current RRM sites are seamlessly transitioned to an intelligent centralized service. AI enhanced RRM along with other Cisco Catalyst Center services brings a host of new features with it.

Cisco AI Enhanced RRM operates as a distributed RRM service. RF telemetry is collected from the Cisco Access Points by the controller, and passed through the Catalyst Center to the Cisco AI Analytics Cloud where the data is stored. The RRM Algorithms run against this telemetry data stored in the cloud. AI analyzes the solutions, and passes any configuration change information back to the Catalyst Center. The Catalyst Center maintains the control connection with the enrolled controller and passes any individual AP configuration changes back to the APs.

The following RRM algorithms run in the cloud while the remaining work in the controller:

- DCA
- TPC
- DBS
- FRA

Note The RRM algorithms run in the cloud against the telemetry data available in the cloud.

If the location of controller, and APs are provisioned previously, assigning a location enrolls the AI Enhanced RRM Services and the profile to be pushed to the controller. Thus, AI Enhanced RRM becomes the RF Group Leader for the subscribed controller.

For more information on the Cisco Catalyst Center, see Cisco Catalyst Center User Guide.

Note The following table covers the controller and Cisco Catalyst Center release versions that support Cisco AI Enhanced RRM support:

Table 39: Controller and Cisco Catalyst Center Releases Supporting Cisco AI Enhanced RRM Support

Controller Release	Cisco Catalyst Center Release	Cisco AI Enhanced RRM Support
Cisco IOS XE Cupertino 17.9.x	• Cisco Catalyst Center, Release 2.3.2 or Cisco Catalyst Center, Release 2.3.3 • Cisco Catalyst Center, Release 2.3.4	• 2.4GHz and 5GHz • 2.4GHz, 5GHz, and 6GHz
Cisco IOS XE Cupertino 17.8.x	• Cisco Catalyst Center, Release 2.3.2 Cisco Catalyst Center, Release 2.3.3 • Cisco Catalyst Center, Release 2.3.4	2.4GHz and 5GHz
Cisco IOS XE Cupertino 17.7.x	Cisco Catalyst Center, Release 2.3.2 or Cisco Catalyst Center, Release 2.3.3	2.4GHz and 5GHz

Restrictions for Radio Resource Management

- The number of APs in a RF-group is limited to 3000.
- If an AP tries to join the RF-group that already holds the maximum number of APs it can support, the device rejects the application and throws an error.
- Disabling all data rates for default rf-profile or custom rf-profile, impacts ISSU upgrade and client join process after the software upgrade (ISSU or non-ISSU). To prevent this, you must enable at least one data rate (for example, **ap dot11 24 rate RATE_5_5M enable**) on the default rf-profile or custom rf-profile. We recommend that you enable the lowest data rate if efficiency is of prime concern.
- Keywords such as secure cannot be used a RF group name.

How to Configure RRM

Configuring Neighbor Discovery Type (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **Radio Resource Management** page, click either the **5 GHz Band**, **2.4 GHz Band** or the **6 GHz Band** tab.

Step 3 In the **General** tab, under each section enter the corresponding field details:

a) Under the **Profile Threshold For Traps** section, enter the:

1. **Interference Percentage**: The foreign interference threshold is between 0 and 100 %. The default is 10 %.
2. **Clients**: The client threshold between 1 and 75 clients. The default is 12.
3. **Noise**: The foreign noise threshold between –127 dBm and 0dBm. The default is –70 dBm.
4. **Utilization Percentage**: The RF utilization threshold between 0 and 100 %. The default is 80 %.
5. **Throughput**: The average rate of successful messages delivery over a communication channel. Value ranges from 1000 to 1000000 bps.

b) Under the **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels** section, choose the:

1. **Channel List** from the drop-down list:
   - All Channels
   - Country Channels
   - DCA Channels
2. **RRM Neighbor Discover Type** from the drop-down list:
   - **Transparent**: Packets are sent as is.
   - **Protected**: Packets are protected.
3. **RRM Neighbor Discovery Mode**:
   - **AUTO**: If the NDP mode configured is AUTO, the controller selects On-Channel as the NDP mode. The default is set as AUTO.
   - **OFF-CHANNEL**: If the NDP mode configured is Off-Channel, the controller selects Off-Channel as the NDP mode.

c) Under the **Monitor** section, set:

- **Neighbor Packet Frequency (seconds)**: Frequency (in seconds) in which the Neighbor Discovery Packets are sent. The default is 180 seconds.
- **Reporting Interval (seconds)**: The default is 180 seconds. Each channel dwell has to be completed within 180 seconds.
- **Neighbor Timeout factor**: Value in seconds used to determine when to prune access points from the neighbor list that have timed out. The default is 20 seconds.

Step 4 Click Apply to save your configuration.

Configuring Neighbor Discovery Type (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 {24ghz | 5ghz | 6ghz} rrm ndp-type** {**protected | transparent**}
	Example:
	`Device(config)#ap dot11 24ghz rrm ndp-type protected`
	`Device(config)#ap dot11 24ghz rrm ndp-type transparent`
		Configures the neighbor discovery type. By default, the mode is set to “transparent”.
		• **protected**: Sets the neighbor discover type to protected. Packets are encrypted.
		• **transparent**: Sets the neighbor discover type to transparent. Packets are sent as is.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RF Groups

This section describes how to configure RF groups through either the GUI or the CLI.

Note When the multiple-country feature is being used, all controllers intended to join the same RF group must be configured with the same set of countries, configured in the same order.

Configuring RF Group Selection Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **RRM** page, click the relevant band's tab: either **6 GHz Band**, **5 GHz Band**, or **2.4 GHz Band**.

Step 3 Click the **RF Grouping** tab.

Step 4 Choose the appropriate **Group Mode** from these options:

- Automatic: Sets the 802.11 RF group selection to automatic update mode
- Leader: Sets the 802.11 RF group selection to leader mode
- Off: Disables the 802.11 RF group selection

Note When AI Enhanced RRM is enabled on a controller and Cisco Catalyst Center is connected to a wireless network, Cisco Catalyst Center is assigned the group role as a leader. Controllers, managed by Cisco Catalyst Center and enabled with AI Enhanced RRM, are assigned the group role as remote members irrespective of the group mode they were previously assigned. The **Group Role** field will display as **Remote Member** and the **Group leader** field will display the IP address of the Cisco Catalyst Center.

Step 5 Save the configuration.

Configuring RF Group Selection Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz | 6ghz} rrm group-mode**{**auto | leader | off**} **Example:** `Device(config)#ap dot11 24ghz rrm group-mode leader`	Configures RF group selection mode for 802.11 bands. • **auto**: Sets the 802.11 RF group selection to automatic update mode. • **leader**: Sets the 802.11 RF group selection to leader mode. • **off**: Disables the 802.11 RF group selection.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RF Group Name (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless rf-network** *name* **Example:** `Device (config)# wireless rf-network test1`	Creates an RF group. The group name should be ASCII String up to 19 characters and is case sensitive. **Note** Repeat this procedure for each controller that you want to include in the RF group.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Secure RF Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless rf-network secure** **Example:** `Device(config)# wireless rf-network secure`	Creates a secure RF group.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 4	**show ap dot11 {24ghz | 5ghz | 6ghz} group** **Example:** `Device# show ap dot11 24ghz group`	Displays configuration and statistics of 6-GHz band grouping.

Configuring Members in an 802.11 Static RF Group (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **RRM** page, click either the **6 GHz Band**, **5 GHz Band** or **2.4 GHz Band** tab.

Step 3 Click the **RF Grouping** tab.

Step 4 Choose the appropriate **Group Mode** from the following options:

- **Automatic(default)**: Members of an RF group elect an RF group leader to maintain a primary power and channel scheme for the group. The RF grouping algorithm dynamically chooses the RF group leader and ensures that an RF group leader is always present. Group leader assignments can and do change (for instance, if the current RF group leader becomes inoperable or if RF group members experience major changes).
- **Leader**: A device as an RF group leader, manually. In this mode, the leader and the members are manually configured and are therefore fixed. If the members are unable to join the RF group, the reason is indicated. The members' management IP addresses and system name are used to request the member to join the leader. The leader tries to establish a connection with a member every 1 minute if the member has not joined in the previous attempt.
- **Off**: No RF group is configured.

Step 5 Under **Group Members** section, click **Add**.

Step 6 In the **Add Static Member** window that is displayed, enter the controller name and the IPv4 or IPv6 address of the controller.

Step 7 Click **Save & Apply to Device**.

Configuring Members in an 802.11 Static RF Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz | 6ghz} rrm group-member** *group_name ip_addr* **Example:** `Device(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1`	Configures members in a 802.11 static RF group. The group mode should be set as leader for the group member to be active.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Transmit Power Control

Configuring Transmit Power (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **6 GHz Band**, **5 GHz Band**, or **2.4 GHz Band** tab, click the **TPC** tab.

Step 3 Choose of the following dynamic transmit power assignment modes:

- *Automatic*(default): The transmit power is periodically updated for all APs that permit this operation.
- *On Demand*: The transmit power is updated on demand. If you choose this option, you get to view the **Invoke Power Update Once**. Click **Invoke Power Update Once** to apply the RRM data successfully.
- *Fixed*: No dynamic transmit power assignments occur and values are set to their global default.

Step 4 Enter the maximum and minimum power level assignment on this radio. If you configure maximum transmit power, RRM does not allow any access point attached to the device to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection). For example, if you configure a maximum transmit power of 11 dBm, then no access point would transmit above 11 dBm, unless the access point is configured manually. The range is –10 dBm to 30 dBm.

Step 5 In the **Power Threshold** field, enter the cutoff signal level used by RRM when determining whether to reduce an access point's power.

The default value for this parameter varies depending on the TPC version you choose. For TPCv1, the default value is –70 dBm, and for TPCv2, the default value is –67 dBm. The default value can be changed when access points are transmitting at higher (or lower) than desired power levels. The range for this parameter is –80 to –50 dBm.

Increasing this value (between –65 and –50 dBm) causes the access points to operate at higher transmit power rates. Decreasing the value has the opposite effect. In applications with a dense population of access points, it may be useful to decrease the threshold to –80 or –75 dBm in order to reduce the number of BSSIDs (access points) and beacons seen by the wireless clients. Some wireless clients might have difficulty processing a large number of BSSIDs or a high beacon rate and might exhibit problematic behavior with the default threshold.

Step 6 Click **Apply**.

Configuring the Tx-Power Control Threshold (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm tpc-threshold** *threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm tpc-threshold -60`	Configures the Tx-power control threshold used by RRM for auto power assignment. The range is from –80 to –50.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the Tx-Power Level (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz} rrm txpower** {*trans_power_level* | **auto** | **max** | **min** | **once**} **Example:** `Device(config)#ap dot11 24ghz rrm txpower auto`	Configures the 802.11 tx-power level • **trans_power_level**—Sets the transmit power level. • **auto**—Enables auto-RF. • **max**—Configures the maximum auto-RF tx-power. • **min**—Configures the minimum auto-RF tx-power. • **once**—Enables one-time auto-RF.
Step 3	**ap dot11 6ghz rrm txpower** *trans_power_level* **auto** **Example:** `Device(config)#ap dot11 6ghz rrm txpower auto`	Configures the 802.11 6-GHz tx-power level. • *trans_power_level*: Sets the transmit power level. Valid values range from 1 to 5. • **auto**: Enables auto-RF.

	Command or Action	Purpose
		Note The 6-GHz band uses constant-PSD instead of constant-EIRP, which allows the transmission at higher power as channel width increases. The power levels are derived based on the configured channel width. At the higher power levels between 1-3, these power values exceed the limit for legacy rate frames, like beacons. As a result, there is no change in the beacon power for higher levels, unlike the 2.4-GHz and 5-GHz bands.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring 802.11 RRM Parameters

Configuring Advanced 802.11 Channel Assignment Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 In the **DCA** tab, choose a **Channel Assignment Mode** to specify the DCA mode:

- *Automatic*(default)—Causes the device to periodically evaluate and, if necessary, update the channel assignment for all joined APs.
- *Freeze*—Causes the device to evaluate and update the channel assignment for all joined APs. If you choose this option, you get to view the Invoke Channel Update Once. Click **Invoke Channel Update Once** to apply the RRM data successfully.
- *Off*—Turns off DCA and sets all AP radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios.

Step 3 From the **Interval** drop-down list, choose the interval that tells how often the DCA algorithm is allowed to run. The default interval is 10 minutes.

Step 4 From the **AnchorTime** drop-down list, choose a number to specify the time of day when the DCA algorithm must start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

Step 5 Check the **Avoid Foreign AP Interference** check box to cause the device's RRM algorithms to consider 802.11 traffic from foreign APs (those not included in your wireless network) when assigning channels to

lightweight APs, or uncheck it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign APs. By default, this feature is in enabled state.

Step 6 Check the **Avoid Cisco AP Load** check box to cause the device's RRM algorithms to consider 802.11 traffic from Cisco lightweight APs in your wireless network when assigning channels. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. By default, this feature is in disabled state.

Step 7 Check the **Avoid Non-802.11a Noise** check box to cause the device's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight APs. For example, RRM may have APs avoid channels with significant interference from non-AP sources, such as microwave ovens. By default, this feature is in enabled state.

Step 8 Check the **Avoid Persistent Non-Wi-Fi Interference** check box to enable the device to take into account persistent non-Wi-Fi interference in DCA calculations. A persistent interfering device is any device from the following categories, which has been seen in the past 7 days - Microwave Oven, Video Camera, Canopy, WiMax Mobile, WiMax Fixed, Exalt Bridge. With **Avoid Persistent Non-Wi-Fi Interference** enabled, if a Microwave Oven is detected, that interference from the Microwave Oven is taken into account in the DCA calculations for the next 7 days. After 7 days, if the interfering device is not detected anymore, it is no longer considered in the DCA calculations.

Step 9 From the **DCA Channel Sensitivity** drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- *Low*—The DCA algorithm is not particularly sensitive to environmental changes. The DCA threshold is 30 dB.
- *Medium* (default)—The DCA algorithm is moderately sensitive to environmental changes. The DCA threshold is 15 dB.
- *High* —The DCA algorithm is highly sensitive to environmental changes. The DCA threshold is 5 dB.

Step 10 Set the **Channel Width** as required. You can choose the RF channel width as 20 MHz, 40 MHz, 80 MHz, 160 MHz, or Best. This is applicable only for 802.11a/n/ac (5 GHZ) radio.

Step 11 The **Auto-RF Channel List** section shows the channels that are currently selected. To choose a channel, check the corresponding check box.

Note If you disable the serving radio channel of the root AP from the **Auto-RF Channel List**, you will not be able to view the neighboring APs in the root APs.

Step 12 In the **Event Driven RRM** section, check the **EDRRM** check box to run RRM when CleanAir-enabled AP detects a significant level of interference. If enabled, set the sensitivity threshold level at which the RRM is invoked, enter the custom threshold, and check the **Rogue Contribution** check box to enter the rogue duty-cycle.

Step 13 Click **Apply**.

Configuring Advanced 802.11 Channel Assignment Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**} **Example:** `Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures CleanAir event-driven RRM parameters. • **High**–Specifies the most sensitivity to non-Wi-Fi interference as indicated by the air quality (AQ) value. • **Low**–Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value. • **Medium**–Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.

Step 3	**ap dot11 6ghz rrm channel dca** {**anchor-time** *0-23* | **global auto** | **interval** *0-24* | **sensitivity** {**high** | **low** | **medium**}}
	Example:
	`Device(config)#ap dot11 6ghz rrm channel dca interval 2`
		Configures 802.11 6GHz dynamic channel assignment algorithm parameters.
		• **anchor-time**–Configures the anchor time for the DCA. The range is between 0 and 23 hours.
		• **global**–Configures the DCA mode for all 802.11 Cisco APs.
		  • **auto**–Enables auto-RF.
		• **interval**–Configures the DCA interval value. The values are 1, 2, 3, 4, 6, 8, 12 and 24 hours and the default value 0 denotes 10 minutes.
		• **sensitivity**–Configures the DCA sensitivity level to changes in the environment.
		  • **high**–Specifies the most sensitivity.
		  • **low**–Specifies the least sensitivity.
		  • **medium**–Specifies medium sensitivity.

	Command or Action	Purpose
Step 4	**ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80** | **best**} **Example:** `Device(config)#ap dot11 5ghz rrm channel dca chan-width best`	Configures the DCA channel bandwidth for all 802.11 radios in the 5-GHz band. Sets the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz, ; 20 MHz is the default value for channel bandwidth. 80 MHz is the default value for best. Set the channel bandwidth to best before configuring the constraints.
Step 5	**ap dot11 5ghz rrm channel dca chan-width width-max** {**WIDTH_20MHz** | **WIDTH_40MHz** | **WIDTH_80MHz** | **WIDTH_MAX**} **Example:** `Device(config)#ap dot11 5ghz rrm channel dca chan-width width-max WIDTH_80MHz`	Configures the maximum channel bandwidth that can be assigned to a channel. In this example, *WIDTH_80MHz* assigns the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz but not greater than that.
Step 6	**ap dot11 6ghz rrm channel dca chan-width width-max** {**WIDTH_20MHz** | **WIDTH_40MHz** | **WIDTH_80MHz** | **WIDTH_MAX**} **Example:** `Device(config)#ap dot11 6ghz rrm channel dca chan-width width-max WIDTH_80MHz`	Configures the maximum channel bandwidth that can be assigned to a channel. In this example, *WIDTH_80MHz* assigns the channel bandwidth to 20 MHz, 40 MHz, or 80 MHz but not greater than that.
Step 7	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** **Example:** `Device(config)#ap dot11 24ghz rrm channel device`	Configures the persistent non-Wi-Fi device avoidance in the 802.11 channel assignment.
Step 8	**ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign** **Example:** `Device(config)#ap dot11 24ghz rrm channel foreign`	Configures the foreign AP 802.11 interference avoidance in the channel assignment.
Step 9	**ap dot11** {**24ghz** | **5ghz**} **rrm channel load** **Example:** `Device(config)#ap dot11 24ghz rrm channel load`	Configures the Cisco AP 802.11 load avoidance in the channel assignment.

	Command or Action	Purpose
Step 10	**ap dot11** {**24ghz** | **5ghz**} **rrm channel noise** **Example:** `Device(config)#ap dot11 24ghz rrm channel noise`	Configures the 802.11 noise avoidance in the channel assignment.
Step 11	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11 Coverage Hole Detection (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM** to configure Radio Resource Management parameters for 802.11ax (6-GHz), 802.11a/n/ac (5-GHz) and 802.11b/g/n (2.4-GHz) radios.

Step 2 On the **Radio Resource Management** page, click **Coverage** tab.

Step 3 To enable coverage hole detection, check the **Enable Coverage Hole Detection** check box.

Step 4 In the **Data Packet Count** field, enter the number of data packets.

Step 5 In the **Data Packet Percentage** field, enter the percentage of data packets.

Step 6 In the **Data RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 7 In the **Voice Packet Count** field, enter the number of voice data packets.

Step 8 In the **Voice Packet Percentage** field, enter the percentage of voice data packets.

Step 9 In the **Voice RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 10 In the **Minimum Failed Client per AP** field, enter the minimum number of clients on an AP with a signal-to-noise ratio (SNR) below the coverage threshold. Value ranges from 1 to 75 and the default value is 3.

Step 11 In the **Percent Coverage Exception Level per AP** field, enter the maximum desired percentage of clients on an access point's radio operating below the desired coverage threshold and click **Apply**. Value ranges from 0 to 100% and the default value is 25%.

Configuring 802.11 Coverage Hole Detection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 2	**ap dot11 {24ghz | 5ghz | 6ghz} rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**}
	Example:
	`Device(config)#ap dot11 24ghz rrm coverage`
	`data fail-percentage 60`
		Configures the 802.11 coverage hole detection for data packets.
		• **fail-percentage**: Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.
		• **rssi-threshold**: Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm.

Step 3	**ap dot11 6ghz rrm coverage data**{**fail-percentage** *fail-percentage-value* | **packet-count** *packet-count-value*}
	Example:
	`Device(config)#ap dot11 6ghz rrm coverage`
	`data fail-percentage 60`
		Configures the 802.11 6-GHz coverage hole detection for data packets.
		• **fail-percentage**: Configures the 802.11 6-GHz coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 6-GHz coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.

Step 4	**ap dot11 {24ghz | 5ghz} rrm coverage exception global** *exception level*
	Example:
	`Device(config)#ap dot11 24ghz rrm coverage`
	`exception global 50`
		Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.

Step 5	**ap dot11 {24ghz | 5ghz} rrm coverage level global** *cli_min exception level*
	Example:
	`Device(config)#ap dot11 24ghz rrm coverage`
	`level global 10`
		Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.

Step 6	**ap dot11 {24ghz | 5ghz | 6ghz} rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} **Example:**	Configures the 802.11 coverage hole detection for voice packets. • **fail-percentage**: Configures the 802.11 coverage failure-rate threshold for uplink

	Command or Action	Purpose
	`Device(config)#ap dot11 24ghz rrm coverage` `voice packet-count 10`	voice packets as a percentage that ranges from 1 to 100%. • **packet-count**: Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255. • **rssi-threshold**: Configures the 802.11 minimum receive coverage level for voice packets that range from –90 to –60 dBm.

Step 7	**ap dot11 6ghz rrm coverage voice**{**fail-percentage** *fail-percentage-value* | **packet-count** *packet-count-value*}
	Example:
	`Device(config)#ap dot11 6ghz rrm coverage`
	`voice packet-count 10`
		Configures the 802.11 6-GHz coverage hole detection for voice packets.
		• **fail-percentage**: Configures the 802.11 6-GHz coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 6-GHz coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.

Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11 Event Logging (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 24ghz | 5ghz | 6ghz rrm logging**{**channel** | **coverage** | **foreign** | **load** | **noise** | **performance** | **txpower**}
	Example:
	`Device(config)#ap dot11 24ghz rrm logging channel`
	`Device(config)#ap dot11 24ghz rrm logging coverage`
		Configures event-logging for various parameters.
		• **channel**—Configures the 802.11 channel change logging mode.
		• **coverage**—Configures the 802.11 coverage profile logging mode.
		• **foreign**—Configures the 802.11 foreign interference profile logging mode.

	Command or Action	Purpose

	`Device(config)#ap dot11 24ghz rrm logging foreign`
	`Device(config)#ap dot11 24ghz rrm logging load`
	`Device(config)#ap dot11 24ghz rrm logging noise`
	`Device(config)#ap dot11 24ghz rrm logging performance`
	`Device(config)#ap dot11 24ghz rrm logging txpower`
		• **load**—Configures the 802.11 load profile logging mode.
		• **noise**—Configures the 802.11 noise profile logging mode.
		• **performance**—Configures the 802.11 performance profile logging mode.
		• **txpower**—Configures the 802.11 transmit power change logging mode.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11 Statistics Monitoring (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM** to configure Radio Resource Management parameters for 802.11ax (6-GHz), 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz) radios.

Step 2 In the **Monitor Intervals(60 to 3600secs)** section, proceed as follows:

a) To configure the 802.11 noise measurement interval (channel scan interval), set the **AP Noise Interval**. The valid range is from 60 to 3600 seconds.

b) To configure the 802.11 signal measurement interval (neighbor packet frequency), set the **AP Signal Strength Interval**. The valid range is from 60 to 3600 seconds.

c) To configure the 802.11 coverage measurement interval, set the **AP Coverage Interval**. The valid range is from 60 to 3600 seconds.

d) To configure the 802.11 load measurement, set the **AP Load Interval**. The valid range is from 60 to 3600 seconds.

Step 3 Click **Apply**.

Configuring 802.11 Statistics Monitoring (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor channel-list**{**all | country | dca**} **Example:** `Device(config)#ap dot11 24ghz rrm monitor channel-list all`	Sets the 802.11 monitoring channel-list for parameters such as noise/interference/rogue. • **all**: Monitors all channels. • **country**: Monitor channels used in configured country code. • **dca**: Monitor channels used by dynamic channel assignment.
Step 3	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor coverage** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor coverage 600`	Configures the 802.11 coverage measurement interval in seconds that ranges from 60 to 3600.
Step 4	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor load** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor load 180`	Configures the 802.11 load measurement interval in seconds that ranges from 60 to 3600.
Step 5	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor measurement** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor measurement 360`	Configures the 802.11 measurement interval in seconds that ranges from 60 to 3600.
Step 6	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor neighbor-timeout-factor** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor neighbor-timeout-factor 50`	Configures the 802.11 neighbor timeout-factor in seconds that ranges from 5 to 60.
Step 7	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor reporting** *interval* **Example:** `Device(config)#ap dot11 24ghz rrm monitor reporting 480`	Configures the 802.11 reporting interval in seconds that ranges from 60 to 3600.
Step 8	**ap dot11 {24ghz | 5ghz | 6ghz} rrm monitor rssi-normalization** **Example:**	Configures the 802.11 RRM Neighbor Discovery RSSI normalization.

	Command or Action	Purpose
	`Device(config)#ap dot11 24ghz rrm monitor rssi-normalization`	

Configuring the 802.11 Performance Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join** page, click the name of the profile or click **Add** to create a new one.

Step 3 In the **Add/Edit RF Profile** window, click the **RRM** tab.

Step 4 In the **General** tab that is displayed, enter the following parameters:

a) In the **Interference (%)** field, enter the threshold value for 802.11 foreign interference that ranges between 0 and 100 percent.

b) In the **Clients** field, enter the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.

c) In the **Noise (dBm)** field, enter the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.

d) In the **Utilization(%)** field, enter the threshold value for 802.11 RF utilization that ranges between 0 to 100 percent.

Step 5 Click **Update & Apply to Device**.

Configuring the 802.11 Performance Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm profile clients** *cli_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile clients 20`	Sets the threshold value for 802.11 Cisco AP clients that range between 1 and 75 clients.
Step 3	**ap dot11** {**24ghz** | **5ghz**}**rrm profile foreign** *int_threshold_value* **Example:**	Sets the threshold value for 802.11 foreign interference that ranges between 0 and 100%.

	Command or Action	Purpose
	`Device(config)#ap dot11 24ghz rrm profile foreign 50`	
Step 4	**ap dot11** {**24ghz** | **5ghz**} **rrm profile noise** *for_noise_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile noise -65`	Sets the threshold value for 802.11 foreign noise ranges between –127 and 0 dBm.
Step 5	**ap dot11 6ghz rrm profile customize** **Example:** `Device(config)#ap dot11 6ghz rrm profile customize`	Enables performance profiles.
Step 6	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm profile throughput** *throughput_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile throughput 10000`	Sets the threshold value for 802.11 Cisco AP throughput that ranges between 1000 and 10000000 bytes per second.
Step 7	**ap dot11** {**24ghz** | **5ghz**} **rrm profile utilization** *rf_util_threshold_value* **Example:** `Device(config)#ap dot11 24ghz rrm profile utilization 75`	Sets the threshold value for 802.11 RF utilization that ranges between 0 to 100%.
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring Advanced 802.11 RRM

Enabling Channel Assignment (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 In the **RRM** page, click the relevant band's tab: either **6 GHz Band**, **5 GHz Band** or **2.4 GHz Band**.

Step 3 Click the **DCA** tab

Step 4 In the **Dynamic Channel Assignment Algorithm** section, choose the appropriate **Channel Assignment Mode** from these options:

- Automatic: Sets the channel assignment to automatic.
- Freeze: Locks the channel assignment. Click **Invoke Channel Update Once** to refresh the assigned channels.

Step 5 Click **Apply**.

Enabling Channel Assignment (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel-update** **Example:** `Device# ap dot11 24ghz rrm channel-update`	Enables the 802.11 channel selection update for each of the Cisco access points. **Note** After you enable **ap dot11 {24ghz | 5ghz} rrm channel-update**, a token is assigned for channel assignment in the DCA algorithm.

Restarting DCA Operation

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm dca restart** **Example:** `Device# ap dot11 24ghz rrm dca restart`	Restarts the DCA cycle for 802.11 radio.

Updating Power Assignment Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **Access Points** page, click the AP name from the 5GHz or 2.4 GHz list.

Step 3 In the **Edit Radios** > **Configure** > **Tx Power Level Assignment** section, choose **Custom** from the **Assignment Method** group-down list.

Step 4 Choose the value for **Transmit Power** from the drop-down list.

Step 5 Click **Update & Apply to Device**.

Updating Power Assignment Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm txpower update** **Example:** `Device# ap dot11 24ghz rrm txpower update`	Initiates the update of the 802.11 6-Ghz transmit power for every Cisco AP.

Configuring Rogue Access Point Detection in RF Groups

Configuring Rogue Access Point Detection in RF Groups (CLI)

Before you begin

Ensure that each controller in the RF group has been configured with the same RF group name.

Note The name is used to verify the authentication IE in all beacon frames. If the controller have different names, false alarms will occur.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *Cisco_AP* **mode** {**monitor** | **clear** | **sensor** | **sniffer**} **Example:** `Device# ap name ap1 mode clear`	Perform this step for every access point connected to the controller . Configures the following AP modes of operation: • **monitor**: Sets the AP mode to monitor mode. • **clear**: Resets AP mode to local or remote based on the site. • **sensor**: Sets the AP mode to sensor mode. • **sniffer**: Sets the AP mode to wireless sniffer mode.
Step 2	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**wireless wps ap-authentication** **Example:** `Device (config)# wireless wps ap-authentication`	Enables rogue access point detection.
Step 5	**wireless wps ap-authentication threshold** *value* **Example:** `Device (config)# wireless wps ap-authentication threshold 50`	Specifies when a rogue access point alarm is generated. An alarm occurs when the threshold value (which specifies the number of access point frames with an invalid authentication IE) is met or exceeded within the detection period. The valid threshold range is from 1 to 255, and the default threshold value is 1. To avoid false alarms, you may want to set the threshold to a higher value. **Note** Enable rogue access point detection and threshold value on every controller in the RF group. **Note** If rogue access point detection is not enabled on every controller in the RF group, the access points on the controller with this feature disabled are reported as rogues.

Monitoring RRM Parameters and RF Group Status

Monitoring RRM Parameters

Table 40: Commands for monitoring Radio Resource Management

Commands	Description
show ap dot11 24ghz channel	Displays the configuration and statistics of the 802.11b channel assignment.
show ap dot11 24ghz coverage	Displays the configuration and statistics of the 802.11b coverage.
show ap dot11 24ghz group	Displays the configuration and statistics of the 802.11b grouping.
show ap dot11 24ghz logging	Displays the configuration and statistics of the 802.11b event logging.
show ap dot11 24ghz monitor	Displays the configuration and statistics of the 802.11b monitoring.
show ap dot11 24ghz profile	Displays 802.11b profiling information for all Cisco APs.
show ap dot11 24ghz summary	Displays the configuration and statistics of the 802.11b Cisco APs.
show ap dot11 24ghz txpower	Displays the configuration and statistics of the 802.11b transmit power control.
show ap dot11 5ghz channel	Displays the configuration and statistics of the 802.11a channel assignment.
show ap dot11 5ghz coverage	Displays the configuration and statistics of the 802.11a coverage.
show ap dot11 5ghz group	Displays the configuration and statistics of the 802.11a grouping.
show ap dot11 5ghz logging	Displays the configuration and statistics of the 802.11a event logging.
show ap dot11 5ghz monitor	Displays the configuration and statistics of the 802.11a monitoring.
show ap dot11 5ghz profile	Displays 802.11a profiling information for all Cisco APs.
show ap dot11 5ghz summary	Displays the configuration and statistics of the 802.11a Cisco APs.
show ap dot11 5ghz txpower	Displays the configuration and statistics of the 802.11a transmit power control.

Verifying RF Group Status (CLI)

This section describes the new commands for RF group status.

The following commands can be used to verify RF group status on the .

Table 41: Verifying Aggressive Load Balancing Command

Command	Purpose

show ap dot11 5ghz group	Displays the controller name which is the RF group leader for the 802.11a RF network.
show ap dot11 24ghz group	Displays the controller name which is the RF group leader for the 802.11b/g RF network.
show ap dot11 6ghz group	Displays the controller name which is the RF group leader for the 802.11 6-GHz RF network.

To display the controller as a remote member and part of the AI Enhanced RRM, use the following command:

```
Device# show ap dot11 24ghz group

Radio RF Grouping

RF Group Name : Open-RRM
RF Protocol Version(MIN) : 100(30)
RF Packet Header Version : 2
802.11b Group Mode : AUTO
802.11b Group Role : Remote-Member
802.11b Group Update Interval : 600 seconds
802.11b Group Leader : 172.19.30.39 (172.19.30.39)
Secure-RRM : Disabled


RF Group Members

Controller name Controller IP Controller IPv6 DTLS status
-----------------------------------------------------------------------------------------------------------
evwlc-188         192.1.0.188     N/A
```

Examples: RF Group Configuration

This example shows how to configure RF group name:

```
Device# configure terminal
Device(config)# wireless rf-network test1
Device(config)# ap dot11 24ghz shutdown
Device(config)# end
Device # show network profile 5
```

This example shows how to configure rogue access point detection in RF groups:

```
Device# ap name ap1 mode clear
Device# end
Device# configure terminal
Device(config)# wireless wps ap-authentication
Device(config)# wireless wps ap-authentication threshold 50
Device(config)# end
```

Information About ED-RRM

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a

threshold for air quality (AQ) that, if exceeded, triggers an immediate channel change for the affected access point. Once a channel change occurs due to event-driven RRM, the channel is blocked list for three hours to avoid selection. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active.

Configuring ED-RRM on the Cisco Wireless Controller (CLI)

Procedure

Step 1 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event** —Configures CleanAir driven RRM parameters for the 802.11 Cisco lightweight access points.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}—Configures CleanAir driven RRM sensitivity for the 802.11 Cisco lightweight access points. Default selection is Medium.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event custom-threshold** *custom-threshold-value*—Triggers the ED-RRM event at the set threshold value. The custom threshold values range from 1 to 99.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution**—Enables rogue contribution.

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution duty-cycle** *thresholdvalue*—Configures threshold value for rogue contribution. The valid range is from 1 to 99, with 80 as the default.

Step 2 Save your changes by entering this command:

write memory

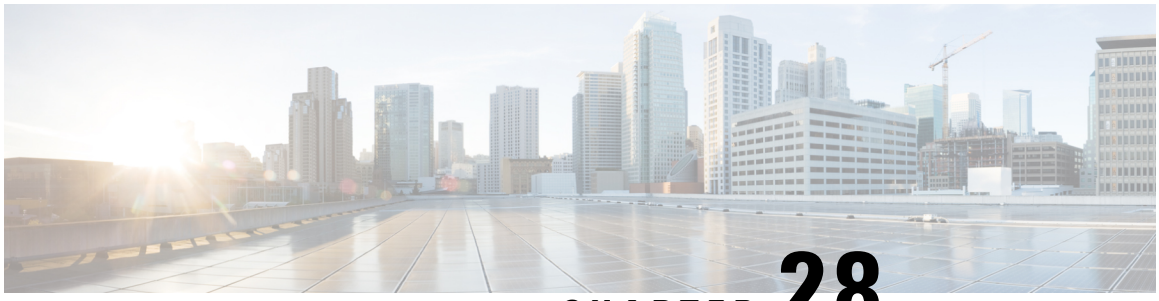
Step 3 See the CleanAir configuration for the 802.11a/n/ac or 802.11b/g/n network by entering this command:

show ap dot11 {**24ghz** | **5ghz**} **cleanair config**

Information similar to the following appears:

```
CleanAir Solution................................ : Enabled
Air Quality Settings:
Air Quality Reporting........................ : Enabled
Air Quality Reporting Period (min)........... : 15
Air Quality Alarms........................... : Disabled
Air Quality Alarm Threshold.................. : 10
Unclassified Interference.................... : Disabled
Unclassified Severity Threshold.............. : 35
Interference Device Settings:
Interference Device Reporting................ : Enabled
BLE Beacon.............................. : Enabled
Bluetooth Link........................... : Enabled
Microwave Oven........................... : Enabled
802.11 FH................................ : Enabled
Bluetooth Discovery...................... : Enabled
TDD Transmitter.......................... : Enabled
```

```
Jammer.................................. : Enabled
Continuous Transmitter.................. : Enabled
DECT-like Phone......................... : Enabled
Video Camera............................ : Enabled
802.15.4................................ : Enabled
WiFi Inverted........................... : Enabled
WiFi Invalid Channel.................... : Enabled
SuperAG................................. : Enabled
Canopy.................................. : Enabled
Microsoft Device........................ : Enabled
WiMax Mobile............................ : Enabled
WiMax Fixed............................. : Enabled
Interference Device Types Triggering Alarms:
BLE Beacon.............................. : Disabled
Bluetooth Link.......................... : Disabled
Microwave Oven.......................... : Disabled
802.11 FH............................... : Disabled
Bluetooth Discovery..................... : Disabled
TDD Transmitter......................... : Disabled
Jammer.................................. : Disabled
Continuous Transmitter.................. : Disabled
DECT-like Phone......................... : Disabled
Video Camera............................ : Disabled
802.15.4................................ : Disabled
WiFi Inverted........................... : Enabled
WiFi Invalid Channel.................... : Enabled
SuperAG................................. : Disabled
Canopy.................................. : Disabled
Microsoft Device........................ : Disabled
WiMax Mobile............................ : Disabled
WiMax Fixed............................. : Disabled
Interference Device Alarms.................. : Disabled
AdditionalClean Air Settings:
CleanAir Event-driven RRM State............. : Disabled
CleanAir Driven RRM Sensitivity............. : LOW
CleanAir Driven RRM Sensitivity Level....... : 35
CleanAir Event-driven RRM Rogue Option...... : Disabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
CleanAir Persistent Devices state........... : Disabled
CleanAir Persistent Device Propagation...... : Disabled
```



CHAPTER 28

Coverage Hole Detection

• Coverage Hole Detection and Correction, on page 527

Coverage Hole Detection and Correction

The RRM coverage hole detection algorithm can detect areas of radio coverage in a wireless LAN that are below the level needed for robust radio performance. This feature can alert you to the need for an additional (or relocated) lightweight access point.

If clients on a lightweight access point are detected at threshold levels (RSSI, failed client count, percentage of failed packets, and number of failed packets) lower than those specified in the RRM configuration, the access point sends a “coverage hole” alert to the device. The alert indicates the existence of an area where clients are continually experiencing poor signal coverage, without having a viable access point to which to roam. The device discriminates between coverage holes that can and cannot be corrected. For coverage holes that can be corrected, the device mitigates the coverage hole by increasing the transmit power level for that specific access point. The device does not mitigate coverage holes caused by clients that are unable to increase their transmit power or are statically set to a power level because increasing their downstream transmit power might increase interference in the network.

Configuring Coverage Hole Detection (GUI)

Follow the procedure given below to configure client accounting.

Procedure

Step 1 Click **Configuration** > **Radio Configurations** > **RRM**.

On this page, you can configure Radio Resource Management parameters for 802.11a/n/ac (5 GHZ) and 802.11b/g/n (2.4 GHZ) radios, and flexible radio assignment parameters.

Step 2 Check the **Enable Coverage Hole Detection** check box.

Enables coverage hole detection.

Configuring Coverage Hole Detection (CLI)

Coverage Hole Detection (CHD) is based on upstream RSSI metrics observed by the AP.

Note To revert back radios from 5-GHz to 24-GHz for CHD, ensure that the 5-GHz radio is UP and Client Network Preference value is other than the default.

Follow the procedure given below to configure CHD:

Before you begin

Disable the 802.11 network before applying the configuration.

Procedure

	Command or Action	Purpose
Step 1	**ap dot11 {24ghz | 5ghz} rrm coverage** **Example:** `Device(config)# ap dot11 24ghz rrm coverage`	Configures the 802.11 coverage level for data packets. Use the **no** form of the command to disable CHD.

Step 2	**ap dot11 {24ghz | 5ghz} rrm coverage data** {**fail-percentage | packet-count | rssi-threshold**}
	Example:
	`Device(config)# ap dot11 24ghz rrm coverage`
	`data fail-percentage 60`
		Configures the 802.11 coverage level for data packets.
		• **fail-percentage**: Configures the 802.11 coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.
		• **rssi-threshold**: Configures the 802.11 minimum receive coverage level for data packets that range from –90 to –60 dBm.

Step 3	**ap dot11 6ghz rrm coverage data**{**fail-percentage** *fail-percentage-value* | **packet-count** *packet-count-value*}
	Example:
	`Device(config)# ap dot11 6ghz rrm coverage`
	`data fail-percentage 60`
		Configures the 802.11 6-GHz coverage hole detection for data packets.
		• **fail-percentage**: Configures the 802.11 6-GHz coverage failure-rate threshold for uplink data packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 6-GHz coverage minimum failure count threshold for uplink data packets that ranges from 1 to 255.

	Command or Action	Purpose

Step 4	**ap dot11 {24ghz | 5ghz} rrm coverage exception global** *exception level*
	Example:
	`Device(config)# ap dot11 24ghz rrm coverage`
	`exception global 50`
		Configures the 802.11 Cisco AP coverage exception level as a percentage that ranges from 0 to 100%.

Step 5	**ap dot11{24ghz | 5ghz}rrm coverage level global** *cli_min exception level*
	Example:
	`Device(config)# ap dot11 24ghz rrm coverage`
	`level global 10`
		Configures the 802.11 Cisco AP client minimum exception level that ranges from 1 to 75 clients.

Step 6	**ap dot11 {24ghz | 5ghz} rrm coverage voice** {**fail-percentage | packet-count | rssi-threshold**}
	Example:
	`Device(config)# ap dot11 24ghz rrm coverage`
	`voice packet-count 10`
		Configures the 802.11 coverage hole detection for voice packets.
		• **fail-percentage**: Configures the 802.11 coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.
		• **rssi-threshold**: Configures the 802.11 minimum receive coverage level for voice packets that range from –90 to –60 dBm.

Step 7	**ap dot11 6ghz rrm coverage voice**{**fail-percentage** *fail-percentage-value* | **packet-count** *packet-count-value*}
	Example:
	`Device(config)# ap dot11 6ghz rrm coverage`
	`voice packet-count 10`
		Configures the 802.11 6-GHz coverage hole detection for voice packets.
		• **fail-percentage**: Configures the 802.11 6-GHz coverage failure-rate threshold for uplink voice packets as a percentage that ranges from 1 to 100%.
		• **packet-count**: Configures the 802.11 6-GHz coverage minimum failure count threshold for uplink voice packets that ranges from 1 to 255.

Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
Step 9	**show ap dot11 {24ghz | 5ghz | 6ghz} coverage** **Example:** `Device# show ap dot11 5ghz coverage`	Displays the CHD details.

Note If both the number and percentage of failed packets exceed the values entered in the **packet-count** and **fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes. False positives are generally due to the poor roaming logic implemented on most clients. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **coverage level global** and **coverage exception global** commands over a 90-second period. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

Configuring CHD for RF Tag Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 On the **Coverage** tab, select the **Enable Coverage Hole Detection** check box.

Step 3 In the **Data Packet Count** field, enter the number of data packets.

Step 4 In the **Data Packet Percentage** field, enter the percentage of data packets.

Step 5 In the **Data RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 6 In the **Voice Packet Count** field, enter the number of voice data packets.

Step 7 In the **Voice Packet Percentage** field, enter the percentage of voice data packets.

Step 8 In the **Voice RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 dBm to -90 dBm; the default value is –80 dBm.

Step 9 In the **Minimum Failed Client per AP** field, enter the minimum number of clients on an AP with a signal-to-noise ratio (SNR) below the coverage threshold. Value ranges from 1 to 75 and the default value is 3.

Step 10 In the **Percent Coverage Exception Level per AP** field, enter the maximum desired percentage of clients on an access point's radio operating below the desired coverage threshold and click Apply. Value ranges from 0 to 100% and the default value is 25%.

Step 11 Click **Apply**.

Configuring CHD for RF Profile (CLI)

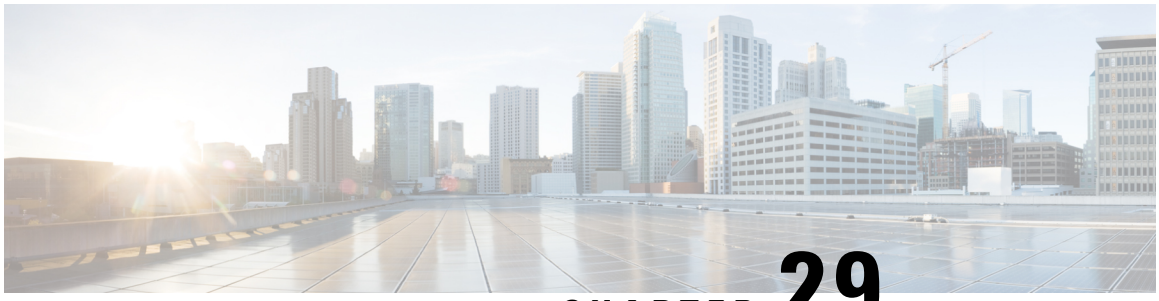
Follow the procedure given below to configure Coverage Hole Detection (CHD) for RF profile.

Before you begin

Ensure that the RF profile is already created.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rf-profile** *rf-profile-tag* **Example:** `Device(config)# ap dot11 24ghz rf-profile alpha-rfprofile-24ghz`	Configures the 802.11 coverage hole detection for data packets.
Step 3	**coverage data rssi threshold** *threshold-value* **Example:** `Device(config-rf-profile)# coverage data rssi threshold -80`	Configures the minimum RSSI value for data packets received by the access point. Valid values range from -90 to -60 in dBm.
Step 4	**end** **Example:** `Device(config-rf-profile)# end`	Returns to privileged EXEC mode.
Step 5	**show ap dot11 24ghz rf-profile summary** **Example:** `Device# show ap dot11 24ghz rf-profile summary`	Displays summary of the available RF profiles.



CHAPTER 29

Optimized Roaming

- Optimized Roaming, on page 533
- Restrictions for Optimized Roaming, on page 533
- Configuring Optimized Roaming (GUI), on page 534
- Configuring Optimized Roaming (CLI), on page 534

Optimized Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection. This feature disassociates clients based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold. You can disable the data rate option so that only RSSI is used for disassociating clients.

Optimized roaming also prevents client association when the client's RSSI is low. This feature checks the RSSI of the incoming client against the RSSI threshold. This check prevents the clients from connecting to a Wi-Fi network unless the client has a viable connection. In many scenarios, even though clients can hear beacons and connect to a Wi-Fi network, the signal might not be strong enough to support a stable connection.

You can also configure the client coverage reporting interval for a radio by using optimized roaming. The client coverage statistics include data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) pre-alarm failures, retransmission requests, and current data rates.

Optimized roaming is useful in the following scenarios:

- Addresses the sticky client challenge by proactively disconnecting clients.
- Actively monitors data RSSI packets.
- Disassociates client when the RSSI is lower than the set threshold.

This section contains the following subsections:

Restrictions for Optimized Roaming

- You cannot configure the optimized roaming interval until you disable the 802.11a/b network.

- When basic service set (*BSS*) transition is sent to 802.11v-capable clients, and if the clients are not transitioned to other BSS before the disconnect timer expires, the corresponding client is disconnected forcefully. BSS transition is enabled by default for 802.11v-capable clients.
- The Cisco Catalyst 9800 controller increments the 80211v smart roam failed counter while disconnecting the client due to optimized roaming.
- We recommend that you do not use the optimized roaming feature with RSSI low check.

Configuring Optimized Roaming (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

Step 2 On the **Advanced** page, click the relevant band's tab: either **5 GHz Band** or **2.4 GHz Band**.

Step 3 Check the **Optimized Roaming Mode** check box to enable the feature.

Step 4 Choose the required **Optimized Roaming Date Rate Threshold**. The threshold value options are different for 802.11a and 802.11b networks.

Optimized roaming disassociates clients based on the RSSI of the client data packet and data rate. The client is disassociated if the current data rate of the client is lower than the Optimized Roaming Data Rate Threshold.

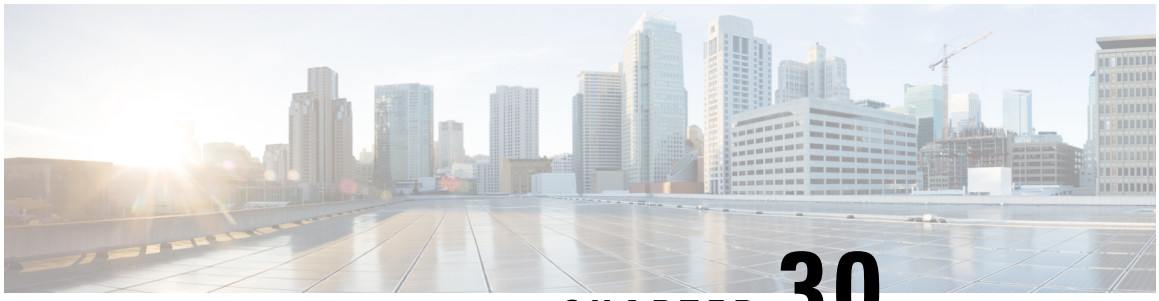
Step 5 Click **Apply** to save the configuration.

Configuring Optimized Roaming (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz | 6ghz} rrm optimized-roam** **Example:** `Device(config)#ap dot11 24ghz rrm optimized-roam`	Configures 802.11a, 802.11b, or 802.11 6-GHz optimized roaming. By default, optimized roaming is disabled.
Step 3	**ap dot11 24ghz rrm monitor optimized-roam data-rate-threshold** {**1M** | **2M** | **5_5M** | **6M** | **9M** | **11M** | **12M** | **18M** | **24M** | **36M** | **48M** | **54M** | **disable**}	Configure the data rate threshold for 802.11b for optimized roaming.

	Command or Action	Purpose
	Example: `Device(config)#ap dot11 24ghz rrm monitor optimized-roam 18M`	
Step 4	**ap dot11 {5ghz | 6ghz} rrm monitor optimized-roam data-rate-threshold** {**6M** | **9M** | **12M** | **18M** | **24M** | **36M** | **48M** | **54M** | **disable**} **Example:** `Device(config)#ap dot11 6ghz rrm monitor optimized-roam 18M`	Configure the data rate threshold for 802.11a or 802.11 6-GHz optimized roaming.
Step 5	**show ap dot11 {24ghz | 5ghz | 6ghz} optimized-roaming statistics** **Example:** `Device#show ap dot11 24ghz optimized-roaming statistics`	Displays the 802.11a, 802.11b, or 802.11 6-GHz optimized roaming configurations.



CHAPTER 30

Cisco Flexible Radio Assignment

- Information About Flexible Radio Assignment, on page 537
- Configuring an FRA Radio (GUI), on page 538
- Enabling FRA (CLI), on page 540
- Configuring Client FRA in RF Profile (CLI), on page 542
- Verifying FRA XOR 5-GHz and 6-GHz Details, on page 542
- Flexible Radio Assignment (FRA) Action, on page 543

Information About Flexible Radio Assignment

Flexible Radio Assignment (FRA) takes advantage of Cisco FRA-capable APs whose radio hardware can operate in multiple roles. The following are the AP models and types of hardware managed by FRA:

Table 42: AP Models and Types of Hardware Managed by FRA

AP Model	FRA Radios	Functions
Cisco Aironet 2800 Series Access Points	2.4/5 XOR	2.4-GHz and 5-GHz or dual 5-GHz operations
Cisco Aironet 3800 Series Access Points	2.4/5 XOR	2.4-GHz and 5-GHz or dual 5-GHz operations
Cisco Aironet 4800 Series Access Points	2.4/5 XOR	2.4-GHz and 5-GHz or dual 5-GHz operations
Cisco Catalyst 9120 Series Access Points	2.4/5 XOR	2.4-GHz and 5-GHz or dual 5-GHz operations
Cisco Catalyst 9130AX Series Access Points	5-GHz Tri-Radio	2.4-GHz 4x4 and single 5-GHz 8x8, or 2.4-GHz 4x4 and dual 5-GHz 4x4
Cisco Catalyst Wireless 9166 Access Points	5/6-GHz XOR	2.4-GHz 4x4 and dual 5-GHz 4x4, or 5-GHz 4x4 and 6-GHz 4x4

FRA performs a number of functions. On the 2.4-GHz and 5-GHz XOR models, FRA establishes the required 2.4-GHz coverage, identifies redundant radios, and converts them to either 5-GHz or a monitor role. For

tri-radio and 5/6-GHz XOR models, FRA determines the 2.4-GHz coverage, and the redundant radios are converted to a monitor role. Additionally, FRA determines the best operating role for the 5-GHz tri-radio (as either a single 8x8 or a dual 4x4), based on connected client capabilities. For the 5/6-GHz XOR radio, the band that the radios should operate on is based on the availability 6-GHz client presence in the regulatory domain.

FRA also manages the resulting configurations of the radios to optimize client experience across flexible roles. Client Steering is responsible for load balancing client connections. For instance, from Cisco Aironet 2800 APs through Cisco Catalyst 9120 Series APs, all the internal antenna AP models perform dual 5-GHz roles as a Macro-Micro cell (a cell within a cell). The antennas on these models are built to support the directionality needed for the micro cell. FRA client steering helps to steer clients to the appropriate radio based on their position within the cell (closer clients are put on the micro cell).

The FRA APs that support external antennas operate as Macro-Macro, which allows full control over power and channels. The CW9166I AP also supports a Macro-Macro model when using the internal antennas.

In Cisco Catalyst 9130 APs and Cisco Catalyst 9136 APs, FRA also manages the operating mode of the band-locked 8x8 5-GHz tri-radio by monitoring client capabilities of connected clients. For instance, if the attached clients are largely Wi-Fi 5-capable clients, then, beam forming should be multi-user MIMO (MU-MIMO), ensuring better capacity with dual 4x4 5-GHz cells. However, if the same cell has a higher number of Wi-Fi 6-capable clients, then 8x8 spatial streams support more MU-MIMO capacity and increase the overall performance of the cell and client experience.

The CW9166 AP is the first AP with a dual-band XOR radio covering the 5-GHz and 6-GHz bands. Criteria for role selection is regulatory domain (that is, if the country's regulatory rules support 6-GHz operations). If yes, 6-GHz is chosen. If not, 5-GHz operations are chosen.

Configuration choices for all FRA radio models include:

- Automatic (Allows FRA to manage role selection automatically)
- Client Serving (Manual role selection of 2.4-GHz, 5-GHz, or 6-GHz, or FRAs are not engaged)
- Monitor (Manual: no FRA)
- Sniffer (Manual: no FRA)

Configuring an FRA Radio (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM** > **FRA**.

Step 2 In the **Flexible Radio Assignment** window, in the **5/6 GHz Flexible Radio Assignment** section, perform the following steps:

a) Click the **FRA Status** toggle button to change the FRA status to **Enabled**. By default, the FRA status is **Disabled**.

b) Click the **FRA Freeze** toggle button to enable FRA freeze. Enable **FRA Freeze** to lock the radio's current assigned role. When enabled, the radios continue to operate in their role (monitor, sniffer or client serving) until you manually change it or disable FRA Freeze.

c) From the **FRA Interval** drop-down list, choose the FRA run interval. The interval value range is from 1 hour to 24 hours. You can choose the FRA run interval value only after you enable the FRA status.

Step 3 In the **2.4/5 GHz Flexible Radio Assignment** section, perform the following steps:

a) Click the **FRA Status** toggle button to change the FRA status to **Enabled**. By default, the FRA status is **Disabled**.

b) Click the **FRA Freeze** toggle button to enable FRA freeze. Enable **FRA Freeze** to lock the radio's current assigned role. When enabled, the radios continue to operate in their role (monitor, sniffer or client serving) until you manually change it or disable FRA Freeze.

c) From the **FRA Interval** drop-down list, choose the FRA run interval. The interval value range is from 1 hour to 24 hours. You can choose the FRA run interval value only after you enable the FRA status.

d) From the **FRA Sensitivity** drop-down list, choose the percentage of Coverage Overlap Factor (COF) required to consider a radio as redundant. You can select the supported value only after you enable the FRA status.

The supported values are as follows:

- **Low**: 100 percent
- **Medium** (default): 95 percent
- **High**: 90 percent
- **Higher**: 85 percent
- **Even Higher**: 80 percent
- **Super High**: 50 percent

e) From the **FRA Action** drop-down list, select the **2.4GHz Monitor** option to globally configure the redundant dual-band (XOR 2.4/5-GHz) radios to operate in monitor role.

By default, dual-band radios operate in the 2.4-GHz/5-GHz/Monitor role. This configuration is helpful especially when there is enough coverage on the 5-GHz band and you want to restrict radios from moving to the 5-GHz band to prevent further interference. Instead, the radios directly move to the monitor mode in the 2.4-GHz band.

f) Check the **Client Aware** check box to take decisions on redundancy.

When enabled, the **Client Aware** feature monitors the dedicated 5-GHz radio. When the client load passes a preset threshold, the Flexible Radio assignment is automatically changed from a monitor role to a 5-GHz role, effectively doubling the capacity of the cell on demand. After the capacity crisis is over and Wi-Fi load returns to normal, the radios resume their previous roles.

g) In the **Client Select** field, enter a value for client selection. The valid value range is between 0 and 100 percent. The default value is 50 percent.

This means that if the dedicated 5-GHz interface reaches 50 percent channel utilization, it triggers the monitor role dual-band interface to transition to a 5-GHz client-serving role.

h) In the **Client Reset** field, enter a reset value for the client. The valid value range is between 0 and 100 percent. The default value is 5 percent.

When the AP is operating as a dual 5-GHz AP, this setting indicates the reduction in the combined radios' overall channel utilization required to reset the dual-band radio to monitor role.

Step 4 Click **Apply** to save the configuration.

Enabling FRA (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**[no] ap fra** **Example:** `Device(config)# [no] ap fra`	Enables or disables FRA on the AP.
Step 3	**[no] ap fra 5-6ghz** **Example:** `Device(config)# ap fra 5-6ghz`	Enables FRA 5-GHz or 6-GHz on APs that support XOR (5-GHz or 6-GHz). Use the **no** form of this command to disable this feature.
Step 4	**[no] ap fra freeze** **Example:** `Device(config)# ap fra freeze`	Enables FRA freeze. Use the **no** form of this command to disable this feature.
Step 5	**[no] ap fra 5-6ghz freeze** **Example:** `Device(config)# ap fra 5-6ghz freeze`	Enables FRA 5-GHz or 6-GHz freeze. Use the **no** form of this command to disable this feature.
Step 6	**ap fra interval** **Example:** `Device(config)# ap fra interval 3`	Configures the FRA interval, in hours. The range is from 1 to 24 hours. **Note** The FRA interval must be more than the configured RRM interval.
Step 7	**ap fra 5-6ghz interval** *number-of-hours* **Example:** `Device(config)# ap fra 5-6ghz interval 4`	Configures the FRA 5-GHz or 6-GHz interval, in hours. The valid range is from 1 to 24 hours.
Step 8	**ap fra sensitivity** {**high** | **medium** | **low**} **Example:** `Device(config)# ap fra sensitivity high`	Configures FRA sensitivity. • **high**: Sets the FRA Coverage Overlap Sensitivity to **high**. • **medium**: Sets the FRA Coverage Overlap Sensitivity to **medium**. • **low**: Sets the FRA Coverage Overlap Sensitivity to **low**.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 10	**ap fra revert** {**all** | **auto-only**}{**auto** | **static**} **Example:** `Device# ap fra revert all auto`	Rolls back the XOR radio state. • **all**: Reverts all XOR Radios • **auto-only**: Reverts only XOR radios that are currently in automatic band selection. • **auto**: Places the XOR radios in automatic band selection. • **static**: Places the XOR radios in static 2.4-GHz, 5-GHz, and 6-GHz bands.
Step 11	(Optional) **show ap dot11** {**24ghz** | **5ghz** | **6ghz** | **dual-band**} **summary** **Example:** `Device# show ap dot11 6ghz summary`	Shows the configuration and statistics of 802.11 Cisco APs.

Step 12	(Optional) **show ap fra**
	Example:
	`Device# show ap fra`
	
	`FRA State`
	`: Disabled`
	`FRA Sensitivity`
	`: medium (95%)`
	`FRA Interval`
	`: 1 Hour(s)`
	
	`AP Name MAC Address`
	`Slot ID Current-Band COF %`
	`Suggested Mode`
	`---`
	`AP00A6.CA36.295A 006b.f09c.8290`
	`0 2.4GHz None`
	`2.4GHz`
	
	`COF : Coverage Overlap Factor`
	
	`test_machine#`
		Shows the current FRA configuration.

Step 13	(Optional) **show ap fra 5-6ghz**	Shows the FRA 5-GHz - 6-GHz configurations.
Step 14	(Optional) **show ap name** *ap-name* **config dot11** {**24ghz** | **5ghz** | **6ghz** | **dual**} **Example:** `Device# show ap name config dot11 6ghz`	Shows the current 802.11 parameters in a given AP.

Configuring Client FRA in RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 6ghz rf-profile** *rf-profile-name* **Example:** `Device(config)# ap dot11 6ghz rf-profile rf-profile-name`	Configures the RF profile and enters RF profile configuration mode.
Step 3	**client-aware-fra client-count-reset** *client-count* **Example:** `Device(config-rf-profile)# client-aware-fra client-count-reset 1`	Configures the client count threshold for the radio to switch from 6-GHz to 5-GHz band. The valid range is from 1 to 10 clients.
Step 4	**client-aware-fra client-reset-util** *util-percentage* **Example:** `Device(config-rf-profile)# client-aware-fra client-reset-util 5`	Configures the utilization threshold for the radio to switch from 6-GHz to 5-GHz band. The valid range is from 0 to 100 percent.

Verifying FRA XOR 5-GHz and 6-GHz Details

To view the FRA 5-GHz and 6-GHz configuration details, run the following command:

```
Device# show ap fra 5-6ghz
```

To view the client utilization threshold and client reset count, run the following command:

```
Device# show ap rf-profile name default-rf-profile-6ghz detail
Description                     : default rfprofile for 6GHz radio
RF Profile Name                 : default-rf-profile-6ghz
Band                            : 6 GHz
Transmit Power Threshold v1     : -70 dBm
Min Transmit Power              : -10 dBm
Max Transmit Power              : 30 dBm
Operational Rates
  802.11 6GHZ 6M Rate               : Mandatory
  802.11 6GHZ 9M Rate               : Supported
  802.11 6GHZ 12M Rate              : Mandatory
  802.11 6GHZ 18M Rate              : Supported
  802.11 6GHZ 24M Rate              : Mandatory
  802.11 6GHZ 36M Rate              : Supported
  802.11 6GHZ 48M Rate              : Supported
  802.11 6GHZ 54M Rate              : Supported
```

```
Max Clients                        : 200
.
.
.
PSC Channel List                   : 5,21,37,53,69,85,101,117,133,149,165,181,197,213,229
DCA Bandwidth                      : best
DCA Foreign AP Contribution        : Enabled
State                              : Up
  Client utilization threshold  : 5%
  Client Reset count            : 1
Client Network Preference          : default
802.11ax
  OBSS PD                          : Disabled
  Non-SRG OBSS PD Maximum          : -62 dBm
  SRG OBSS PD                      : Disabled
  SRG OBSS PD Minimum              : -82 dBm
  SRG OBSS PD Maximum              : -62 dBm
  Broadcast Probe Response         : Disabled
  FILS Discovery                   : Disabled
  Multi-BSSID Profile Name         : default-multi-bssid-profile
NDP mode                           : Auto
Guard Interval                     : none
PSC Enforcement                    : Disabled
```

Note The **client utilization threshold** is the utilization threshold for radios to switch from 6-GHz to 5-GHz band. The **client reset count** is the client count threshold for radios to switch from 6-GHz to 5-GHz band.

Flexible Radio Assignment (FRA) Action

Feature History for Flexible Radio Assignment Action

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 43: Feature History for FRA Action

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Flexible Radio Assignment (FRA) Action	In Cisco IOS-XE 17.10.1 and earlier releases, the FRA moves the redundant dual-band radios to either 5-GHz client-serving role or monitor role.
Cisco IOS XE Dublin17.11.1	Flexible Radio Assignment (FRA) Action	From Cisco IOS-XE 17.11.1 onwards, you can select the redundant dual-band radios in a network to operate in monitor only mode.

Information About Flexible Radio Assignment Action

Flexible Radio Assignment (FRA) evaluates only 2.4-GHz radio coverage and determines whether there is overlapping coverage that is causing radio interference. If there is an overlapping coverage, the dual-band radio moves to either 5-GHz client serving or monitor role.

In Cisco IOS-XE 17.10.1 and earlier releases, the FRA moves the redundant dual-band radios to either 5-GHz client-serving role or monitor role.

From Cisco IOS-XE 17.11.1 onwards, you can select the redundant dual-band radios in a network to operate in monitor only mode.

Note The FRA action feature is disabled by default.

Configuring FRA Action in Default RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap dot11 24ghz fra action monitor** **Example:** `Device(config)# ap dot11 24ghz fra action monitor`	Configures the FRA action as monitor, and moves all redundant dual-band radios to monitor role only.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuring FRA Action in 2.4-GHz RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap dot11 24ghz rf-profile** *rf-profile-tag* **Example:**	Configures the RF profile name and enters RF profile configuration mode.

	Command or Action	Purpose
	`Device(config)# ap dot11 24ghz rf-profile alpha-rfprofile-24ghz`	
Step 3	**fra action monitor** **Example:** `Device(config-rf-profile)# fra action monitor`	Configures the FRA action as monitor, and moves all redundant dual-band radios to monitor role only.
Step 4	**end** **Example:** `Device(config-rf-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying FRA Action Configuration

To view the selected FRA action, use the following command:

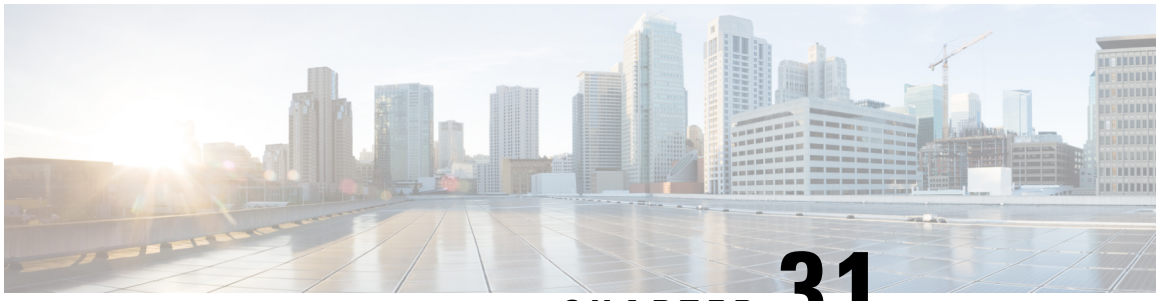
```
Device# show ap fra
FRA State              : Enabled
FRA Freeze             : Disabled
FRA Operation State    : Up
FRA Sensitivity        : higher (85%)
FRA Interval           : 1 Hour(s)
Service Priority       : Coverage
Client Aware FRA       : Enabled
  Client Select        : 25%
  Client Reset         : 5%
FRA Action             : 2.4GHz/Monitor
  Last Run             : 3069 seconds ago
```

To view the FRA action details in an AP RF profile, use the following command:

```
Device# show ap rf-profile name madhu-rf-profile-24 detail | sec FRA
Client Aware FRA                  : Disabled
FRA Action                        : 2.4GHz/Monitor
```

To view the radio mode and role in an AP, use the following command:

```
Device# show ap name AP7872.5DED.CB74 config slot 0 | sec Attribute
Attributes for Slot 0
  Radio Type                                    : 802.11n - 2.4/5 GHz
  Radio Mode                                    : Monitor
  Radio Role                                    : Monitor
    Assignment Method                           : Auto
    Monitor Mode Reason                         : Automatically Switched by FRA
```



CHAPTER 31

XOR Radio Support

- Information About Dual-Band Radio Support , on page 547
- Configuring Default XOR Radio Support, on page 548
- Configuring XOR Radio Support for the Specified Slot Number (GUI), on page 550
- Configuring XOR Radio Support for the Specified Slot Number, on page 551

Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in Cisco 2800, 3800, 4800, and the 9120 series AP models offer the ability to serve 2.4–GHz or 5–GHz bands or passively monitor both the bands on the same AP. These APs can be configured to serve clients in 2.4–GHz and 5–GHz bands, or serially scan both 2.4–GHz and 5–GHz bands on the flexible radio while the main 5–GHz radio serves clients.

Cisco Catalyst Wireless 9166 AP (CW9166) now has XOR function for a dual 5-GHz 4x4 or 5-GHz 4x4 and 6-GHz 4x4 radios. These radios can also be configured as client serving, monitor or as a sniffer interface like the earlier XOR radios.

Note For all countries that do not support 6-GHz spectrum for use of Wi-Fi, when the Cisco Catalyst Wireless 9166I AP operates as dual 5-GHz, the 5-GHz channels will be locked on both the radios even if slot 2 is disabled or set up for monitoring.

Cisco APs models up and through the Cisco 9120 APs are designed to support dual 5–GHz band operations with the *i* model supporting a dedicated Macro/Micro architecture and the *e* and *p* models supporting Macro/Macro. The Cisco 9130AXI APs and the Cisco 9136 APs support dual 5-GHz operations as Micro/Messo cell, and the CW9166I supports as Macro/Macro.

When a radio moves between bands (from 2.4-GHz to 5-GHz and vice versa), clients need to be steered to get an optimal distribution across radios. When an AP has two radios in the 5–GHz band, client steering algorithms contained in the Flexible Radio Assignment (FRA) algorithm are used to steer a client between the same band co-resident radios.

The XOR radio support can be steered manually or automatically:

- Manual steering of a band on a radio—The band on the XOR radio can only be changed manually.
- Automatic client and band steering on the radios is managed by the FRA feature that monitors and changes the band configurations as per site requirements.

Note RF measurement will not run when a static channel is configured on slot 1. Due to this, the dual band radio slot 0 will move only with 5–GHz radio and not to the monitor mode.

When slot 1 radio is disabled, RF measurement will not run, and the dual band radio slot 0 will be only on 2.4–GHz radio.

Note Only one of the 5-GHz radios can operate in the UNII band (100 - 144), due to an AP limitation to keep the power budget within the regulatory limit.

Configuring Default XOR Radio Support

Before you begin

Note The default radio points to the XOR radio hosted on slot 0.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* **Example:** `Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	Configures the 802.11 dual-band antenna on a specific Cisco access point. *antenna_gain_value*: The valid range is from 0 to 40.
Step 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** **Example:** `Device# ap name ap-name dot11 dual-band shutdown`	Shuts down the default dual-band radio on a specific Cisco access point. Use the **no** form of the command to enable the radio.
Step 4	**ap name** *ap-name* **dot11 dual-band role manual client-serving** **Example:** `Device# ap name ap-name dot11 dual-band role manual client-serving`	Switches to client–serving mode on the Cisco access point.

	Command or Action	Purpose
Step 5	**ap name** *ap-name* **dot11 dual-band band 24ghz** **Example:** `Device# ap name ap-name dot11 dual-band band 24ghz`	Switches to 2.4-GHz radio band.
Step 6	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} **Example:** `Device# ap name ap-name dot11 dual-band txpower 2`	Configures the transmit power for the radio on a specific Cisco access point. **Note** When an FRA-capable radio (slot 0 on 9120 AP[for instance]) is set to Auto, you cannot configure static channel and Txpower on this radio. If you want to configure static channel and Txpower on this radio, you will need to change the radio role to Manual Client-Serving mode. This note is not applicable for Cisco Catalyst Wireless 9166 AP (CW9166).
Step 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* **Example:** `Device# ap name ap-name dot11 dual-band channel 2`	Enters the channel for the dual band. *channel-number*—The valid range is from 1 to 173.
Step 8	**ap name** *ap-name* **dot11 dual-band channel auto** **Example:** `Device# ap name ap-name dot11 dual-band channel auto`	Enables the auto channel assignment for the dual-band.
Step 9	**ap name** *ap-name* **dot11 dual-band channel width**{**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} **Example:** `Device# ap name ap-name dot11 dual-band channel width 20 MHz`	Chooses the channel width for the dual band.
Step 10	**ap name** *ap-name* **dot11 dual-band cleanair** **Example:** `Device# ap name ap-name dot11 dual-band cleanair`	Enables the Cisco CleanAir feature on the dual-band radio.

	Command or Action	Purpose

Step 11	**ap name** *ap-name* **dot11 dual-band cleanair band**{**24 GHz | 5 GMHz**}
	Example:
	`Device# ap name ap-name dot11 dual-band cleanair band 5 GHz`
	`Device# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz`
		Selects a band for the Cisco CleanAir feature.
		Use the **no** form of this command to disable the Cisco CleanAir feature.

Step 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A | B | C | D**} **Example:** `Device# ap name ap-name dot11 dual-band dot11n antenna A`	Configures the 802.11n dual-band parameters for a specific access point.
Step 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** **Example:** `Device# show ap name ap-name auto-rf dot11 dual-band`	Displays the auto-RF information for the Cisco access point.
Step 14	**show ap name** *ap-name* **wlan dot11 dual-band** **Example:** `Device# show ap name ap-name wlan dot11 dual-band`	Displays the list of BSSIDs for the Cisco access point.

Configuring XOR Radio Support for the Specified Slot Number (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** section, select the AP for which you want to configure dual-band radios.

The AP name, MAC address, CleanAir capability and slot information for the AP are displayed. If the Hyperlocation method is HALO, the antenna PID and antenna design information are also displayed.

Step 3 Click **Configure**.

Step 4 In the **General** tab, set the **Admin Status** as required.

Step 5 Set the **CleanAir Admin Status** field to Enable or Disable.

Step 6 Click **Update & Apply to Device**.

Configuring XOR Radio Support for the Specified Slot Number

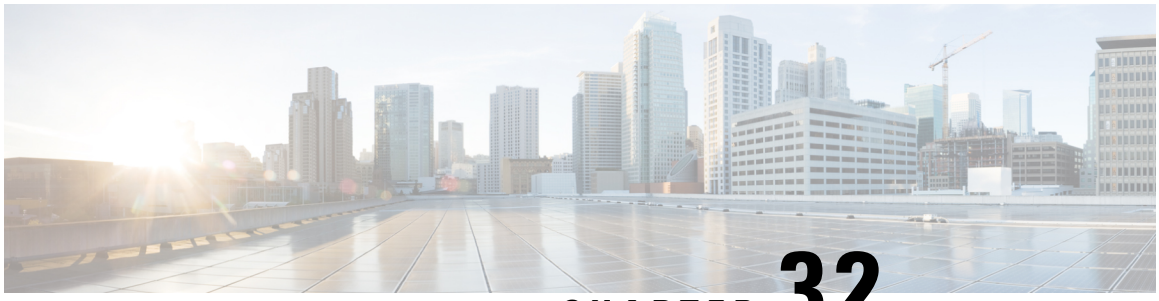
Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point. *external_antenna_gain_value* - Is the external antenna gain value in multiples of .5 dBi unit. The valid range is from 0 to 40. **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model.
Step 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	Configures current band for the XOR radio hosted on slot 0 for a specific access point.
Step 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	Configures dual-band channel for the XOR radio hosted on slot 0 for a specific access point. *channel_number*- The valid range is from 1 to 165.
Step 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} **Example:**	Enables CleanAir features for dual-band radios hosted on slot 0 for a specific access point.

	Command or Action	Purpose
	`Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	
Step 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	Configures 802.11n dual-band parameters hosted on slot 0 for a specific access point. Here, **A**- Enables antenna port A. **B**- Enables antenna port B. **C**- Enables antenna port C. **D**- Enables antenna port D.
Step 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	Configures dual-band role for the XOR radio hosted on slot 0 for a specific access point. The following are the dual-band roles: • **auto**- Refers to the automatic radio role selection. • **manual**- Refers to the manual radio role selection.

Step 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown**
	Example:
	`Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown`
	`Device# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`
		Disables dual-band radio hosted on slot 0 for a specific access point.
		Use the **no** form of this command to enable the dual-band radio.

Step 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	Configures dual-band transmit power for XOR radio hosted on slot 0 for a specific access point. • *tx_power_level*- Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**- Enables auto-RF.



CHAPTER 32

Cisco Receiver Start of Packet

- Information About Receiver Start of Packet Detection Threshold, on page 553
- Restrictions for Rx SOP, on page 553
- Configuring Rx SOP (CLI), on page 554
- Customizing RF Profile (CLI), on page 554

Information About Receiver Start of Packet Detection Threshold

The Receiver Start of Packet (Rx SOP) Detection Threshold feature determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. As the Wi-Fi level increases, the radio sensitivity decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network.

Rx SOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points. Rx SOP helps to optimize the network performance in high-density deployments, such as stadiums and auditoriums where access points need to optimize the nearest and strongest clients.

Restrictions for Rx SOP

- Rx SOP configuration is not applicable to the third radio module pluggable on Cisco Aironet 3600 Series APs.
- Rx SOP configurations are supported only in Local, FlexConnect, Bridge, and Flex+Bridge modes.
- Rx SOP configurations are not supported in the FlexConnect+PPPoE, FlexConnect+PPPoE-wIPS, and FlexConnect+OEAP submodes.

The following table shows the permitted range for the Rx SOP threshold.

Table 44: Rx SOP Threshold

Radio Band	Threshold High	Threshold Medium	Threshold Low
2.4 GHz	-79 dBm	-82 dBm	-85 dBm
5 GHz	-76 dBm	-78 dBm	-80 dBm

Configuring Rx SOP (CLI)

Procedure

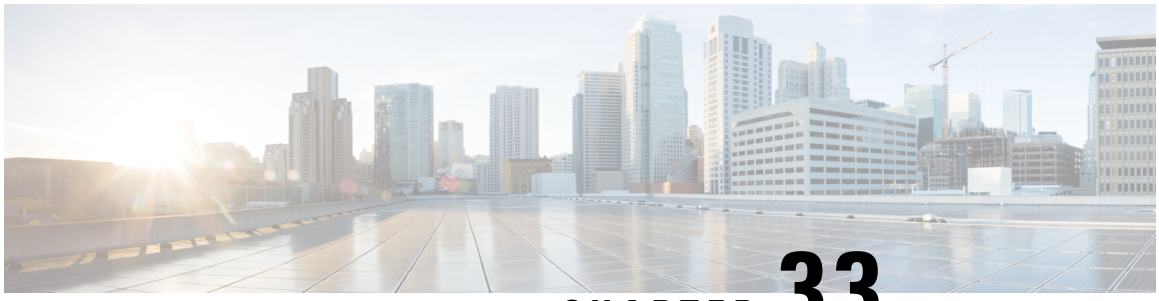
	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {24ghz | 5ghz} rx-sop threshold {auto | custom | high | low | medium}** **Example:** `Device(config)# ap dot11 5ghz rx-sop threshold high`	Configures the 802.11bg/802.11a radio Rx SOP threshold.
Step 3	end	Returns to privileged EXEC mode.
Step 4	**show ap dot11 {24ghz | 5ghz} high-density** **Example:** `Device# show ap dot11 5ghz high-density`	Displays the 802.11bg/802.11a high-density parameters.
Step 5	**show ap summary** **Example:** `Device# show ap summary`	Displays a summary of all the connected Cisco APs.

Customizing RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**high-density rx-sop threshold {auto | custom | high | low | medium}** **Example:** `Device(config-rf-profile)# high-density rx-sop threshold high`	Configures the 802.11bg, 802.11a or 802.11 6-GHz high-density parameters.

	Command or Action	Purpose
Step 3	**show ap summary** **Example:** `Device# show ap summary`	Displays a summary of all the connected Cisco APs.
Step 4	end	Returns to privileged EXEC mode. **Note** • Irrespective of radio mode, the controller configures the radio with configured RX-SOP value. The AP determines whether to use the configured RX-SOP value. • For the XOR radio (Slot 0), when the AP is in monitor mode the RX-SOP value that gets pushed to AP depends on the band it was operating before moving to monitor mode (basically if radio operating band is 24g then RX-SOP params picked from 24GHz RF profile (or default rf-profile). If it was in 5g then RX-SOP params picked from 5GHz RF profile (or default rf-profile) configured for the AP).



CHAPTER 33

Client Limit

- Information About Client Limit, on page 557
- Configuring Client Limit Per WLAN (GUI), on page 557
- Configuring Client Limit Per WLAN (CLI), on page 558
- Configuring Client Limit Per AP (GUI), on page 559
- Configuring Client Limit Per AP (CLI), on page 559
- Configuring Client Limit Per Radio (GUI), on page 560
- Configuring Client Limit Per Radio (CLI), on page 560
- Verifying Client Limit, on page 561

Information About Client Limit

This feature enforces a limit on the number of clients that can to be associated with an AP. Further, you can configure the number of clients that can be associated with each AP radio.

From Cisco IOS XE Cupertino 17.8.x onwards, client limiting is supported per AP, per radio, and per radio per WLAN.

Limitations for Client Limit

- APs other than the Cisco Catalyst 9136 Series APs, support only 200 clients per radio. If you configure more than 200 clients for these APs, the number of clients that can be associated with the AP radios will still be limited to only 200 clients, as per the AP capability value.
- Client limiting is supported on the Cisco Catalyst 9136 Series APs in Flex mode.

Configuring Client Limit Per WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click a WLAN from the list of WLANs.

Step 3 Click the **Advanced** tab.

Step 4 Under the **Max Client Connections** settings, enter the client limit for **Per WLAN**, **Per AP Per WLAN**, and **Per AP Radio Per WLAN**.

Step 5 Click **Update & Apply to Device**.

Configuring Client Limit Per WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name* **Example:** `Device(config)# wlan ramban`	Specifies the WLAN name.
Step 4	**client association limit** *maximum-clients-per-WLAN* **Example:** `Device(config-wlan)# client association limit 110`	Configures the maximum number of clients that can be associated to the given WLAN.
Step 5	**client association limit ap** *max-clients-per-AP-per-WLAN* **Example:** `Device(config-wlan)# client association limit ap 120`	Configures the maximum number of clients that can be associated to an AP in the WLAN. The valid range is between 0 and 1200 clients. The default value is 0. **Note** A Cisco Catalyst 9136 Series AP can support a maximum of 1200 clients.
Step 6	**client association limit radio** *maximum-clients-per-AP-radio-per-WLAN(0—400)* **Example:** `Device(config-wlan)# client association limit radio 100`	Configures the maximum limit of clients that can be associated to an AP radio in the WLAN. The valid range is between 0 to 400 clients. The default value is 200. **Note** A Cisco Catalyst 9136 Series AP radio can support a maximum of 400 clients.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**show wlan id** *wlan-id* **Example:** `Device# show wlan id 2`	Displays the current configuration of the WLAN and the corresponding client association limits.

Configuring Client Limit Per AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the name and description of the corresponding AP join profile.

Step 4 Click the **Client** tab.

Step 5 In the **Maximum Client Limit** field, enter the maximum client associations per AP. The valid values are between 0 and 1200. The default value is 0.

Step 6 Click **Apply to Device**.

Configuring Client Limit Per AP (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**association-limit** *max-client-connections* **Example:**	Configures the maximum client connections per AP. The default value is 0.

	Command or Action	Purpose
	`Device(config-ap-profile)# association-limit 200`	**Note** A Cisco Catalyst 9136 Series AP can support a maximum of 1200 clients.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Client Limit Per Radio (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

Step 2 In the **RF** tab, click the required RF profile name from the displayed list of RF profiles.

The **Edit RF Profile** page is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Under the **High Density Parameters** section, in the **Max Clients** field, enter the maximum number of client connections per AP radio. The valid range is between 0 and 400. The default value is 200 client connections.

Step 5 Click **Update & Apply to Device**.

Configuring Client Limit Per Radio (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rf-profile** *rf-profile-name* **Example:** `Device(config)# ap dot11 6ghz rf-profile rf-profile-name`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**high-density clients count** *maximum-client-connections <0-400>*	Configures the maximum number of client connections per AP radio. The valid range is

	Command or Action	Purpose
	Example: `Device(config-rf-profile)# high-density clients count 200`	between 0 and 400. The default value is 200 client connections. **Note** A Cisco Catalyst 9136 Series AP radio can support a maximum of 400 clients.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

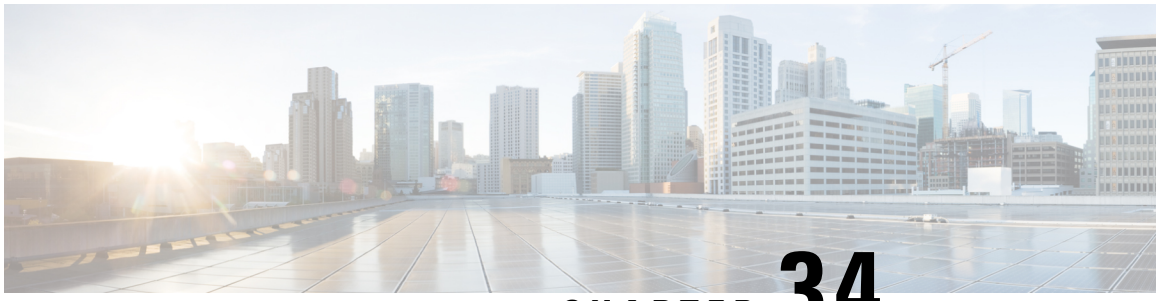
Verifying Client Limit

To verify client limit in local mode, run the following command:

```
Device# show wireless stats client delete reasons | sec Max
Maximum client limit reached on AP                  : 0
Maximum client limit reached on AP per wlan         : 0
Maximum client limit reached on AP radio per wlan   : 0
Maximum client limit reached on AP radio            : 0
```

To verify client limit in the FlexConnect central authentication mode, run the following command:

```
Device# show wireless stats client delete reasons | sec max
AP limiting maximum client per AP               : 0
AP limiting maximum client per AP radio per wlan : 0
AP limiting maximum client per AP radio          : 0
```



CHAPTER 34

IP Theft

- Introduction to IP Theft, on page 563
- Configuring IP Theft (GUI), on page 564
- Configuring IP Theft, on page 564
- Configuring the IP Theft Exclusion Timer, on page 564
- Adding Static Entries for Wired Hosts, on page 565
- Verifying IP Theft Configuration, on page 566

Introduction to IP Theft

The IP Theft feature prevents the usage of an IP address that is already assigned to another device. If the controller finds that two wireless clients are using the same IP address, it declares the client with lesser precedence binding as the IP thief and allows the other client to continue. If blocked list is enabled, the client is put on the exclusion list and thrown out.

The IP Theft feature is enabled by default on the controller. The preference level of the clients (new and existing clients in the database) are also used to report IP theft. The preference level is a learning type or source of learning, such as Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), data glean (looking at the IP data packet that shows what IP address the client is using), and so on. The wired clients always get a higher preference level. If a wireless client tries to steal the wired IP, that client is declared as a thief.

The order of preference for IPv4 clients are:

1. DHCPv4
2. ARP
3. Data packets

The order of preference for IPv6 clients are:

1. DHCPv6
2. NDP
3. Data packets

Note The static wired clients have a higher preference over DHCP.

Configuring IP Theft (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies** > **Client Exclusion Policies**.

Step 2 Check the **IP Theft or IP Reuse** check box.

Step 3 Click **Apply**.

Configuring IP Theft

Follow the procedure given below to configure the IP Theft feature:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps client-exclusion ip-theft** **Example:** `Device(config)# wireless wps client-exclusion ip-theft`	Configures the client exclusion policy.

Configuring the IP Theft Exclusion Timer

Follow the procedure given below to configure the IP theft exclusion timer:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**exclusionlist timeout** *time-in-seconds* **Example:** `Device(config-wireless-policy)# exclusionlist timeout 5`	Specifies the timeout, in seconds. The valid range is from 0-2147483647. Enter zero (0) for no timeout.

Adding Static Entries for Wired Hosts

Follow the procedure given below to create static wired bindings:

Note The statically configured wired bindings and locally configured SVI IP addresses have a higher precedence than DHCP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	Use the first option to configure an IPv4 static entry or the second option to create an IPv6 static entry. • **device-tracking binding vlan** *vlan-id ipv4-address* **interface gigabitEthernet***ge-intf-num hardware-or-mac-address* • **device-tracking binding vlan** *vlan-id ipv6-address* **interface gigabitEthernet***ge-intf-num hardware-or-mac-address* **Example:** `Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1 0000.1111.2222` **Example:**	Configures IPv4 or IPv6 static entry.

	Command or Action	Purpose
	Device(config)# device-tracking binding vlan 20 2200:20:20::6 interface gigabitEthernet 1 0000.444.3333	

Verifying IP Theft Configuration

Use the following command to check if the IP Theft feature is enabled or not:

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures   : Enabled
  Excessive 802.11-authentication failures: Enabled
  Excessive 802.1x-authentication         : Enabled
  IP-theft                                : Enabled
  Excessive Web authentication failure    : Enabled
  Cids Shun failure                       : Enabled
  Misconfiguration failure                : Enabled
  Failed Qos Policy                       : Enabled
  Failed Epm                              : Enabled
```

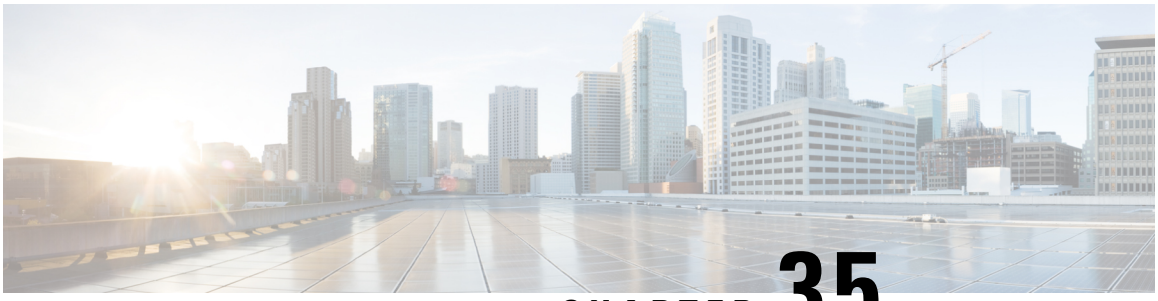
Use the following commands to view additional details about the IP Theft feature:

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method     Role
-------------------------------------------------------------------------------------------
000b.bbb1.0001 SimAP-1                2    Run                11a      None       Local


Number of Excluded Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method
-------------------------------------------------------------------------------------------
10da.4320.cce9 charlie2               2    Excluded           11ac     None


Device# show wireless device-tracking database ip

IP                              VLAN  STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------
  20.20.20.2                     20    Reachable   Local       001e.14cc.cbff
  20.20.20.6                     20    Reachable   IPv4 DHCP   000b.bbb1.0001


Device# show wireless exclusionlist

Excluded Clients

MAC Address       Description          Exclusion Reason               Time Remaining
-------------------------------------------------------------------------------------------
10da.4320.cce9                         IP address theft                    59
```

Note Client exclusion timer deletes the entry from exclusion list with a granularity of 10 seconds. The entry is checked to retain or delete after every 10 seconds. There are chances that the running timer value for excluded clients might display negative values upto 10 seconds.

Note When client exclusion is enabled, it adds the client to the exclusion list. It does not block the client from getting deleted.

```
Device# show wireless exclusionlist client mac 12da.4820.cce9 detail

Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : IP address theft
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```



CHAPTER 35

Unscheduled Automatic Power Save Delivery

- Information About Unscheduled Automatic Power Save Delivery, on page 569
- Viewing Unscheduled Automatic Power Save Delivery (CLI), on page 569

Information About Unscheduled Automatic Power Save Delivery

Unscheduled automatic power save delivery (U-APSD) is a QoS facility that is defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending the battery life, this feature reduces the latency of traffic flow that is delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet that is buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet.

U-APSD is enabled automatically when WMM is enabled.

Viewing Unscheduled Automatic Power Save Delivery (CLI)

Procedure

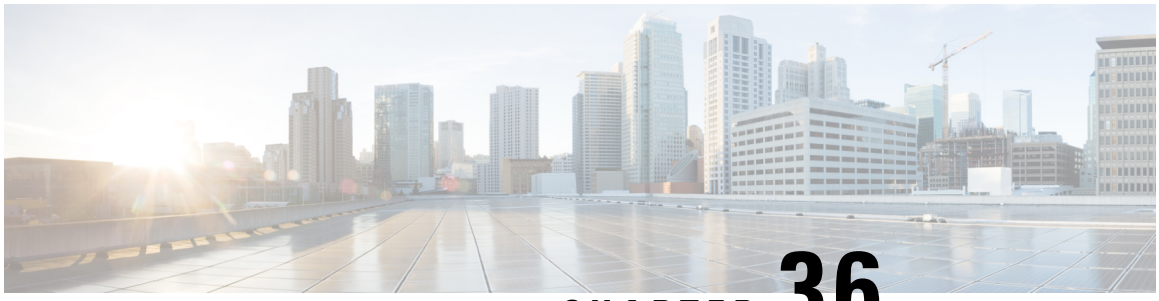
show wireless client mac-address *client_mac* **detail**

Example:

```
Device# show wireless client mac-address 2B:5B:B3:18:56:E9 detail
Output Policy State : Unknown
Output Policy Source : Unknown
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 15
  APSD ACs    : BK(T/D), BE, VI(T/D), VO(T/D)
Power Save : OFF
Current Rate :

--------------------------
BK : Background
BE : Best Effort
VI : Video
VO : Voice.

T: UAPSD Trigger Enabled
```

```
D: UAPSD Delivery Enabled
T/D : UAPSD Trigger and Delivery Enabled
```

Show detailed information of a client by MAC address.



CHAPTER 36

Target Wake Time

- Target Wake Time, on page 571
- Configuring Target Wake Time at the Radio Level (CLI), on page 572
- Configuring Target Wake Time on WLAN, on page 573
- Configuring Target Wake Time (GUI), on page 575
- Verifying Target Wakeup Time, on page 575

Target Wake Time

The existing Wi-Fi client power-saving mechanisms have been in use since 802.11b, where the client devices sleep between AP beacons or multiple beacons, waking up only when they have data to transmit (they can transmit at any time, as AP does not sleep), and beacons containing the Delivery Traffic Indication Map (DTIM), a bit-map, indicates that the AP has downlink traffic buffered for transmission to particular clients.

If a client has a DTIM bit set, it can retrieve data from the AP by sending a Power-Save Poll (PS-Poll) frame to the AP. This power-save scheme is effective but only allows clients to doze for a small beacon interval. Clients still need to wake up several times per second to read DTIM from the beacon frame of the AP.

With 802.11e, the new power-saving mechanism was introduced that helps voice-capable Wi-Fi devices, as voice packets are transmitted at short time intervals, typically 20 ms/sec. Unscheduled automatic power-save delivery (U-APSD) allows a power-save client to sleep at intervals within a beacon period. AP buffers the downlink traffic until the client wakes up and requests its delivery.

Note By default Target Wake Time (TWT) is disabled on the controller. To enable TWT, run the **ap dot11 {24ghz | 5ghz| 6ghz} dot11ax twt-broadcast** command.

Extended Power-Savings Using Target Wake Time

Target wake time (TWT) allows an AP to manage activity in the Wi-Fi network, in order to minimize medium contention between Stations (STAs), and to reduce the required amount of time that an STA in the power-save mode needs to be awake. This is achieved by allocating STAs to operate at non-overlapping times, and/or frequencies, and concentrate the frame exchanges in predefined service periods.

TWT capable STA can either negotiate an individual TWT agreement with TWT-scheduling AP, or it can elect to be part or member of Broadcast TWT agreement existing on the AP. An STA does not need to be

aware that a TWT service period (SP) can be used to exchange frames with other STAs. Frames transmitted during a TWT SP can be carried in any PPDU format supported by the pair of STAs that have established the TWT agreement corresponding to that TWT SP, including High Efficiency Multi-User Physical Protocol Data Unit (HE MU PPDU), High Efficiency Trigger-Based Physical Protocol Data Unit (HE TB PPDU), and so on.

Following are the TWT Agreement Types:

Individual TWT

Single TWT session is negotiated between AP and an STA. This ensures a specific service period of DL and UL between AP and STA with expected traffic to be limited within the negotiated SP of 99% accuracy. The service period starts at specific offset from the target beacon transmission time (TBTT) and runs for the SP duration and repeats every SP interval.

TWT Requesting STA communicates the Wake Scheduling information to its TWT responding AP, which then devises a schedule and delivers the TWT values to the TWT requesting STA when a TWT agreement has been established between them.

Solicited TWT

STA initiates the TWT session with the AP.

Unsolicited TWT

AP initiates TWT setup with STA. AP sends TWT response with service period which is accepted by STA.

Broadcast TWT

High-Efficiency AP requests the STA to participate in the broadcast TWT operation, either on-going broadcast SP or new SP.

Configuring Target Wake Time at the Radio Level (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **shutdown** **Example:** `Device(config)#ap dot11 24ghz shutdown`	Disables the 802.11a, 802.11b, or 802.11 6-GHz network.
Step 3	**ap dot11** {**24ghz** | **5ghz**| **6ghz**} **dot11ax** **Example:** `Device(conf)#ap dot11 24ghz dot11ax`	Configures the 802.11ax parameters. 802.11ax cannot be disabled on the 6-GHz band.
Step 4	**[no] ap dot11** {**24ghz** | **5ghz**| **6ghz**} **dot11ax target-wakeup-time** **Example:**	Configures 802.11 6-GHz dot11ax target wake-up time.

	Command or Action	Purpose
	`Device(config)#ap dot11 24ghz dot11ax target-wakeup-time`	
Step 5	**[no] ap dot11** {**24ghz** | **5ghz** | **6ghz**} **dot11ax twt-broadcast** **Example:** `Device(config)#ap dot11 24ghz dot11ax twt-broadcast`	Configures 802.11 6-GHz dot11ax target wake-up time broadcast. **Note** By default TWT is disabled on the controller. You can enable TWT by running this command.
Step 6	**no ap dot11** {**24ghz** | **5ghz** | **6ghz**} **shutdown** **Example:** `Device(config)#no ap dot11 24ghz shutdown`	Enables the 802.11a or 802.11b network. Enables the 802.11a, 802.11b, or 802.11 6-GHz network.
Step 7	**show ap dot11** {**24ghz** | **5ghz** | **6ghz**} **network** **Example:** `Device(config)#show ap dot11 24ghz network`	Displays the 802.11ax network configuration details, which includes information about Target Wakeup Time and Target Wakeup Broadcast.

Configuring Target Wake Time on WLAN

Enabling Target Wake Time on WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile* **Example:** `Device(config)# wlan wlan-profile`	Enters WLAN configuration submode. The *wlan-profile* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Device(conf-wlan)#shutdown`	Disables the WLAN network
Step 4	**dot11ax target-waketime** **Example:** `Device(conf-wlan)#dot11ax target-waketime`	Configures target wake time mode on WLAN.

	Command or Action	Purpose
Step 5	**dot11ax twt-broadcast-support** **Example:** `Device(conf-wlan)#dot11ax twt-broadcast-support`	Configures the TWT broadcast support on WLAN.
Step 6	**no shutdown** **Example:** `Device(conf-wlan)#no shutdown`	Enables WLAN.

Step 7	**show wlan** {**all** | **id** | **name** | **summary**}
	Example:
	`Device# show wlan all`
	`Device# show wlan id`
	`Device# show wlan name`
		Displays the details of the configured WLAN, including Target Wakeup Time and Target Wakeup Time Broadcast.

Disabling Target Wakeup Time on WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan wlan-profile`	Enters WLAN configuration submode. The *wlan-profile* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Device(conf-wlan)#shutdown`	Disables the WLAN network
Step 4	**no dot11ax target-waketime** **Example:** `Device(conf-wlan)#no dot11ax target-waketime`	Disables the target wake time mode on WLAN.
Step 5	**no dot11ax twt-broadcast-support** **Example:** `Device(conf-wlan)#no dot11ax twt-broadcast-support`	Disables the TWT broadcast support on WLAN.

	Command or Action	Purpose
Step 6	**no shutdown** **Example:** `Device(conf-wlan)#no shutdown`	Enables WLAN.

Configuring Target Wake Time (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **Parameters**.

The parameters page is displayed where you can configure global parameters for 5 GHz Band and 2.4 GHz Band radios.

Step 2 In the **11ax Parameters** section, check the **Target Wakeup Time** check box and the **Target Wakeup Time Broadcast** check box to configure target wakeup time and broadcast target wakeup time.

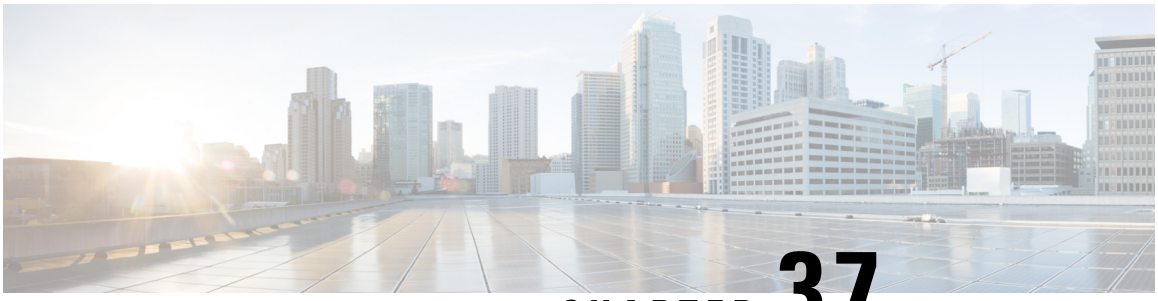
Verifying Target Wakeup Time

To verify Target Wakeup Time and Target Wakeup Time Broadcast, use the following command:

show ap dot11 24ghz network

The following is a sample output:

```
Device#show ap dot11 24ghz network
.
.
.
802.11ax                                : Enabled
Target Wakeup Time                      : Enabled
Target Wakeup Time Broadcast            : Enabled
.
.
.
```



CHAPTER 37

Enabling USB Port on Access Points

- USB Port as Power Source for Access Points, on page 577
- Configuring an AP Profile (CLI), on page 578
- Configuring USB Settings for an Access Point (CLI), on page 579
- Configuring USB Settings for an Access Point (GUI), on page 579
- Monitoring USB Configurations for Access Points (CLI), on page 580

USB Port as Power Source for Access Points

Some Cisco APs have a USB port that can act as a source of power for some USB devices. The power can be up to 2.5W; if a USB device draws more than 2.5W of power, the USB port shuts down automatically. The port is enabled when the power draw is 2.5W and lower. Refer to the datasheet of your AP to check if the AP has a USB port that can act as a source of power.

Note Both IW6300 and ESW6300 APs have a USB port that can act as a source of power up to 4.5W for some USB devices.

Note The controller records the last five power-overdrawn incidents in its logs.

Caution When unsupported USB device is connected to the Cisco AP, the following message is displayed:

```
The inserted USB module is not a supported device. The behavior of this
USB device and the impact to the Access Point is not guaranteed. If Cisco
determines that a fault or defect can be isolated due to the use of
third-party USB modules installed by a customer or reseller, Cisco may
withhold support under warranty or support program under contract. In the
course of providing support for Cisco networking products, the end user
may be required to install Cisco-supported USB modules in the event Cisco
determines that removing third-party parts will assist Cisco in diagnosing
root cause for troubleshooting purposes. Cisco also reserves the right
to charge the customer per then-current time and material rates for
services provided to the customer when Cisco determines, after having
provided such services, that an unsupported device caused the root cause
of the defective product
```

Configuring an AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters the AP profile configuration mode. **Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**usb-enable** **Example:** `Device(config-ap-profile)# usb-enable`	Enables USB for each AP profile. **Note** By default, the USB port on the AP is disabled. Use the **no usb-enable** command to disable USB for each AP profile.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring USB Settings for an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **usb-module** **Example:** `Device# ap name AP44d3.xy45.69a1 usb-module`	Enables the USB port on the AP. Use the **ap name** *ap-name* **no usb-module** command to disable the USB port on the AP. **Note** If you are using Cisco Catalyst 9105AXW AP and if you enable the USB port (.3at PoE-in), it is not possible to enable the USB PoE-out at the same time.
Step 3	**ap name** *ap-name* **usb-module override** **Example:** `Device# ap name AP44d3.xy45.69a1 usb-module override`	Overrides USB status of the AP profile and considers the local AP configuration. Use the **ap name** *ap-name* **no usb-module override** command to override USB status of the AP and consider the AP profile configuration. **Note** You can configure the USB status for an AP only if you enable USB override for it.

Configuring USB Settings for an Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Access Points** window, click the name of the AP.

Step 3 In the **Edit AP** window, click the **Interfaces** tab.

Step 4 In the **USB Settings** section, configure the **USB Module State** as either of the following:

- **ENABLED**: Enables the USB port on the AP
- **DISABLED**: Disables the USB port on the AP

Note If you are using Cisco Catalyst 9105AXW AP and if you enable the USB port (.3at PoE-in), it is not possible to enable the USB PoE-out at the same time.

Step 5 Configure **USB Override** as either of the following:

- **ENABLED**: Overrides USB status of the AP profile and considers the local AP configuration
- **DISABLED**: Overrides USB status of the AP and considers the AP profile configuration

Note You can configure the USB status for an AP only if you enable USB override for it.

Step 6 Click **Apply & Update to Device**.

Monitoring USB Configurations for Access Points (CLI)

- To view the inventory details of APs, use the following command:

  show ap name *ap-name* **inventory**

  The following is a sample output:

```
Device# show ap name AP500F.8059.1620  inventory
NAME: AP2800    , DESCR: Cisco Aironet 2800 Series (IEEE 802.11ac) Access Point
PID: AIR-AP2802I-D-K9  ,  VID: 01,  SN: XXX1111Y2ZZZZ2800
NAME: SanDisk    , DESCR: Cruzer Blade
PID: SanDisk  ,  SN: XXXX1110010, MaxPower: 224
```

- To view the summary of an AP module, use the following command:

  show ap module summary

  The following is a sample output:

```
Device# show ap module summary
AP Name               External Module       External Module PID   External Module
Description
-------------------------------------------------------------------------------------------------
AP500F.1111.2222      Enable                SanDisk               Cruzer Blade
```

- To view the USB configuration details for each AP, use the following command:

  show ap name *ap-name* **config general**

  The following is a sample output:

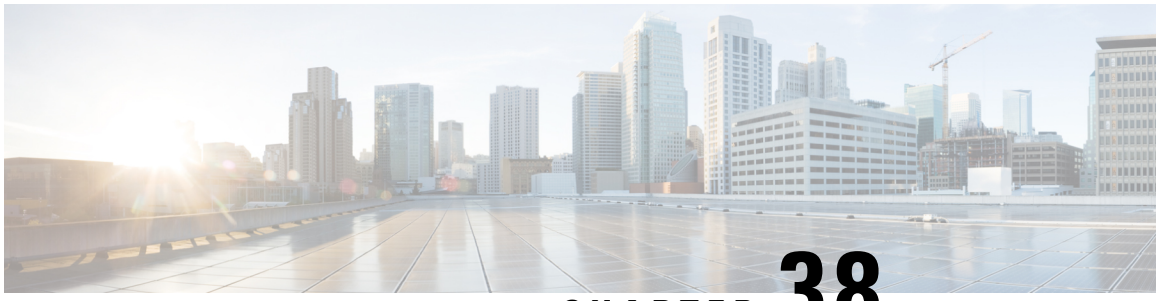
```
Device# show ap name AP500F.111.2222 config general

.
.
.
USB Module Type.................................. USB Module
USB Module Status................................ Disabled
USB Module Operational State..................... Enabled
USB Override ..................................... Enabled
```

- To view status of the USB module, use the following command:

  show ap profile name *xyz* **detailed**

  The following is a sample output:

```
Device# show ap profile name xyz detailed
USB Module               : ENABLED
```



CHAPTER 38

Dynamic Frequency Selection

- Feature History for Channel Availability Check (CAC), on page 581
- Information About Dynamic Frequency Selection, on page 581
- Information About Channel Availability Check (CAC), on page 582
- Verifying DFS, on page 582
- Information About Zero Wait Dynamic Frequency Selection, on page 583
- Configuring Zero Wait Dynamic Frequency Selection Globally (CLI), on page 583
- Configuring Zero Wait Dynamic Frequency Selection Globally (GUI), on page 583
- Enabling Zero Wait Dynamic Frequency Selection on a RF Profile (CLI), on page 584
- Enabling Zero Wait Dynamic Frequency Selection on a RF Profile (GUI), on page 584
- Verifying Zero Wait Dynamic Frequency Selection Configuration, on page 585

Feature History for Channel Availability Check (CAC)

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 45: Feature History for Channel Availability Check (CAC)

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.5.1	Channel Availability Check (CAC)	When a DFS channel is selected for an AP radio, the AP radio scans the channel to check for any radar signals before transmitting any frames in the DFS frequency. This process is called Channel Availability Check (CAC).

Information About Dynamic Frequency Selection

Dynamic Frequency Selection (DFS) is the process of detecting radar signals and automatically setting the frequency on a DFS-enabled 5.0-GHz (802.11a/h) radio to avoid interference with the radar signals. Radios configured for use in a regulatory domain must not interfere with radar systems.

In normal DFS, when a radar signal is detected on any of the channels in the 40-MHz or 80-MHz bandwidth, the whole channel is blocked. With Flex DFS, if the radar signals are not detected on the secondary channel, the AP is moved to a secondary channel with a reduction in the bandwidth, usually, by half.

Information About Channel Availability Check (CAC)

When a DFS channel is selected for an AP radio, the AP radio scans the channel to check for any radar signals before transmitting any frames in the DFS frequency. This process is called Channel Availability Check (CAC).

Note CAC is executed before you set a DFS channel for the radio.

If the AP detects that a radar is using a specific DFS channel, the AP marks the channel as non-available and excludes it from the list of available channels. This state lasts for 30 minutes after which the AP checks again to see, if the channel can be used for Wi-Fi transmissions.

Note

- The CAC performed during a boot process takes anywhere between 1 and 10 minutes depending on the country. This is the reason as to why the DFS channels are not available immediately when an AP reboots.
- APs in the ETSI domain scan channels which are not supported by the controller, as the hardware has the ability to scan.

Verifying DFS

Use the following commands to verify the DFS configuration:

To display the 802.11h configuration, use the following command:

```
Device# show wireless dot11h
```

To display the auto-rF information for 802.11h configuration, use the following command:

```
Device# show ap auto-rf dot11 5ghz
```

To display the auto-rF information for a Cisco AP, use the following command:

```
Device# show ap name ap1 auto-rf dot11 5gh
```

To display the channel details for a Cisco AP, use the following command:

```
Device# show ap dot11 5ghz summary
AP Name Mac Address Slot Admin State Oper State Width Txpwr Channel
-----------------------------------------------------------------------------------------------------------------
pnp-ap 04eb.409e.b560 1 Enabled Up 40 *8/8 (3 dBm) (52,56)
BLDG1-9130-RACK-1568 04eb.409f.11a0 1 Disabled Down 40 4/8 (15 dBm) (100,104)#
```

Note In the show command, # is added right next to the channel whenever CAC is running on an AP radio.

Information About Zero Wait Dynamic Frequency Selection

Access points (APs) monitor and perform Channel Availability Check (CAC) on a potential channel for 60 seconds when AP moves to Dynamic Frequency Selection (DFS) channels. Further, the AP ensures that there is no radar operating in the same frequency range before advertising beacons and serving clients. When the AP moves to a DFS, there is a service outage for a minute. This outage can be higher and extend up to 10 minutes. The Zero Wait Dynamic Frequency Selection feature helps to avoid the service outage in regulatory domains. As of now, U.S. and Europe are the only supported domains.

Configuring Zero Wait Dynamic Frequency Selection Globally (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz rrm channel zero-wait-dfs** **Example:** `Device(config)# ap dot11 5ghz rrm channel zero-wait-dfs`	Enables the Zero Wait Dynamic Frequency Selection feature. By default, the feature is disabled. Use the **no** form of this command to disable the feature. **Note** The Zero Wait Dynamic Frequency Selection feature is only available on a 5-GHz radio.

Configuring Zero Wait Dynamic Frequency Selection Globally (GUI)

Procedure

Step 1 Choose **Configuration > Radio Configurations > RRM**.

Step 2 In the **RRM** page, click the **5 GHz Band** tab.

Step 3 Click the **DCA** tab.

Step 4 Select the **Zero Wait DFS** check box to allow the AP to change to DFS without a service outage.

Step 5 Click **Apply**.

Enabling Zero Wait Dynamic Frequency Selection on a RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz rf-profile** *profile-name* **Example:** `Device(config)# ap dot11 5ghz rf-profile test-dfs`	Configures a radio frequency (RF) profile and enters RF profile configuration mode.
Step 3	**channel zero-wait-dfs** **Example:** `Device(config-rf-profile)# channel zero-wait-dfs`	Enables the Zero Wait Dynamic Frequency Selection feature for the RF profile. Use the **no** form of this command to disable the feature.

Enabling Zero Wait Dynamic Frequency Selection on a RF Profile (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > RF/Radio**.

Step 2 In the **RF** tab, click **Add**.

The **Add RF Profile** page is displayed.

Step 3 Enter the name for the RF profile.

Step 4 From the **Radio Band** drop-down, choose the **5 GHz** band.

Step 5 Click the **RRM** tab.

Step 6 Click the **DCA** tab.

Step 7 Select the **Zero Wait DFS** check box to allow the AP to change to DFS without a service outage.

Step 8 Click **Apply to Device**.

Verifying Zero Wait Dynamic Frequency Selection Configuration

Use the following commands to verify the DFS configuration.

To display the Zero Wait DFS configuration on an AP, use the following command:

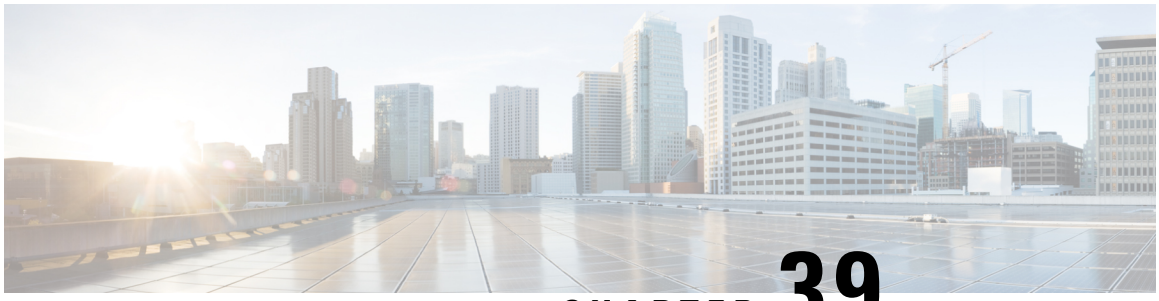
```
Device# show ap name ap1 config slot 1 | inc Zero

  Zero Wait DFS Parameters
    Zero Wait DFS Capable                       : Yes
    CAC Domain                                  : None
```

To display the global configuration related to the Zero Wait Dynamic Frequency Selection feature, use the following command:

```
Device# show ap dot11 5ghz channel | inc Zero

  Zero Wait DFS Parameters
    Zero Wait DFS Capable                       : Yes
    CAC Domain                                  : None
```

To display the RF profile configuration related to the Zero Wait Dynamic Frequency Selection feature, use the following command:

```
Device# show ap rf-profile name test detail | sec Zero

Description                       :
RF Profile Name                   : test
Band                              : 5 GHz
Transmit Power Threshold v1       : -70 dBm
Min Transmit Power                : -10 dBm
Max Transmit Power                : 30 dBm
.
.
.
Guard Interval                    : default
Zero Wait DFS                     : Enabled
```



CHAPTER 39

Cisco Access Points with Tri-Radio

- Cisco Access Points with Tri-Radio, on page 587
- Guidelines and Restrictions for Tri-Radio Access Points, on page 589
- Configuring Tri-Radio, on page 589

Cisco Access Points with Tri-Radio

This topic describes the Tri-Radio feature for Cisco Access Points (APs).

Access Points with three radios are designed for high density environments. The APs by default run one dedicated 2.4-GHz 4x4 mode radio and one 5-GHz 8x8 mode radio. In the default mode, the radios are managed by the Flexible Radio Assignment (FRA), and the Dual Radio Mode is in the disabled state indicating that the radios have either been assigned as client serving 8x8 radio or have not yet been evaluated by FRA.

When you enable the dual radio mode setting, the 8x8 radio is split to two independent 5-GHz 4x4 radios. In this mode, slot 1 and slot 2 are active independent 4x4 radio interfaces. They can serve different user groups with different assigned channels.

Note To disable the dual radio mode, you must first disable the admin status of the subordinate radio. Otherwise, a warning message is displayed.

A tri-radio AP has upto two configurable 5-GHz radios. The following table describes the radio role and its deployment benefits:

In Cisco IOS XE Dublin 17.13.1, the **ap tri-radio** command cannot be configured, since the Tri-radio settings are enabled by default, and cannot be disabled.

Table 46: 5-GHz Radio Operational Modes and Criteria

Radio Role		Driving Factors
Radio 1	**Radio 2**	
8x8 Client-Serving	None	• Preferred operation: 160 MHz or 80 + 80 MHz • Higher MU-MIMO stations • Required higher number of Spatial Streams (SS)
4x4 Client-Serving	4x4 Client-Serving	• Preferred operation: 80 MHz or below • High Capacity in low or medium density • Directional antenna units (Coverage Slicing)
4x4 Client-Serving	4x4 Monitor	• Preferred operation: 80 MHz or below • Lower MU-MIMO stations • Better channel reuse in high density • Monitoring application requires 4x4 Rx

The following table lists the different radio modes and roles supported by the AP:

Table 47: Tri-Radio AP Radio Configuration

Setup	Radio Mode	Maximum Radio Capability	Dual Role Mode
1	2.4-GHz + 5-GHz	2.4-GHz, 4 antennas, 4SS, and 20 MHz 5-GHz, 8 antennas, 4SS, and 160 MHz	Disabled
2	2.4-GHz + 5-GHz	2.4-GHz, 4 antennas, 4SS, and 20 MHz 5-GHz, 8 antennas, 8SS, and 80 MHz	Disabled

Setup	Radio Mode	Maximum Radio Capability	Dual Role Mode
3	2.4-GHz + 5-GHz + 5-GHz	2.4-GHz, 4 antennas, 4SS, and 20 MHz 5-GHz, 4 antennas, 4SS, and 80 MHz 5-GHz, 4 antennas, 4SS, and 80 MHz	Enabled

In the Cisco IOS XE 17.2.1 Release, FRA manages the role assignment for each radio independently. You can set the radio mode as automatic or manual, and select either Client-Serving role or Monitor role as the radio role. Based on the dual radio mode configuration, the role selection is available for one or for both interfaces.

Guidelines and Restrictions for Tri-Radio Access Points

- Dual radio mode is set to **Auto** by default. FRA manages the dual radio mode in **Auto** mode.
- The tri-radio support for AP with external antenna is as follows:
  - RP-TNC antenna is supported in Cisco Catalyst 9130AX Series APs.
  - The C-ANT9101, C-ANT9102, and C-ANT9103 antennas on Cisco Catalyst 9130AX Series APs support 2 radios (2.4-GHz (4x4) and 5-GHz (8x8)). This antennas does not support two 5-GHz (4x4) radios due to hardware limitation.
- From Cisco IOS XE Cupertino 17.7.x, the Tri-Radio feature is supported in Cisco Catalyst 9124 Series APs.

Configuring Tri-Radio

Configuring Tri-Radio for AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **Network**.

The **Network** > **5 GHz Radios** page is displayed.

Step 2 In the **General** section, the **Tri-Radio Mode** check box is enabled by default.

Note You cannot disable the **Tri-Radio Mode** configuration.

Step 3 Click **Apply**

Configuring the Tri-Radio (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	[no] **ap tri-radio** **Example:** `Device(config)# ap tri-radio`	Configures all supporting tri-radio AP's dual radio role in auto mode. Use the **[no]** form of the command to disable the feature.

Configuring 5-GHz Dual Radio Mode for AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **Access Points** page, click the **5 GHz Radios** section and select a Cisco 9130 Series AP from the list. The **Edit Radios 5 GHz Band** window is displayed.

Step 3 In the **Edit Radios 5-GHz Band** > **Configure** > **General** tab, under **Dual Radio Mode**, select one from the following radio button options

- Auto: Permits FRA to decide the mode for this AP.
- Enabled: Enables Dual Radio mode for this AP.
- Disabled: Disables Dual Radio mode for this AP.

Step 4 Click **Update & Apply to Device**.

Configuring the Dual Radio Mode and Enabling Slots (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **dot11 5ghz slot** { **1** | **2** } **shutdown** **Example:** `Device# ap name ap-name dot11 5ghz slot 1 shutdown`	(Optional) Disables the 802.11a radio on Cisco AP.

	Command or Action	Purpose
Step 2	**ap name** *ap-name* **dot11 5ghz slot 1 dual-radio mode** { **disable** | **enable** | **auto** } **Example:** `Device# ap name ap-name dot11 5ghz slot 1 dual-radio mode enable`	Configures the 802.11a dual and tri-radio on the AP. Enable **auto** to allow RRM to switch the AP between dual radio or tri radio mode based on the channel width configuration. In **auto** mode, the slot 2 state is managed by the RRM. Use the **disable** keyword to disable the dual-radio. **Note** When the AP is set to **auto** mode, the dual radio mode is disabled by default.
Step 3	**ap name** *ap-name* **no dot11 5ghz slot** {**1** | **2** } **shutdown** **Example:** `Device# ap name ap-name no dot11 5ghz slot 1 shutdown`	Enables the 802.11a radio on Cisco AP.

Setting Radio Roles for Slots (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**ap name** *ap-name* **dot11** { **24ghz** | **5ghz** | **6ghz** } **slot** <*slot ID*> **radio role** {**auto** | **manual** {**monitor** | **client-serving**}} **Example:** `Device# ap name ap-name dot11 5ghz slot 2 radio role manual monitor`	Sets the radio role manual to either client serving or monitor.

Configuring the Tri-Radio Dual Radio Role (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **dot11 5ghz slot** {**1** | **2** } **radio role** {**auto** | **manual** {**client-serving** | **monitor**} **Example:**	Configures the 802.11a radio role independently for each supporting AP's radio. The channel and the Tx power values can be configured when the radio role is set to **manual** mode.

	Command or Action	Purpose
	`Device# ap name 9130axtrial dot11 5ghz slot 1 radio role manual monitor`	
Step 2	**ap name** *ap-name* **dot11 24ghz slot 0 radio role** {**auto** | **manual** {**client-serving** | **monitor**} **Example:** `Device# ap name 9130axtrial dot11 24ghz slot 0 radio role manual client-serving`	Configures the 802.11b radio role independently for the supporting AP's radio.

Verifying Tri-Radio Configuration on the Controller

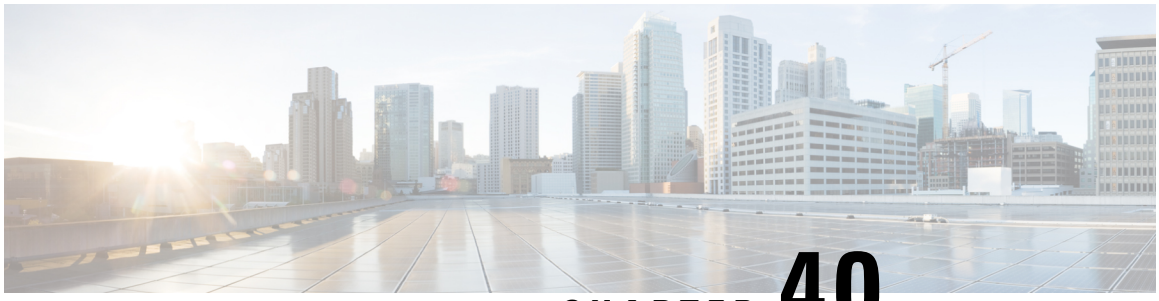
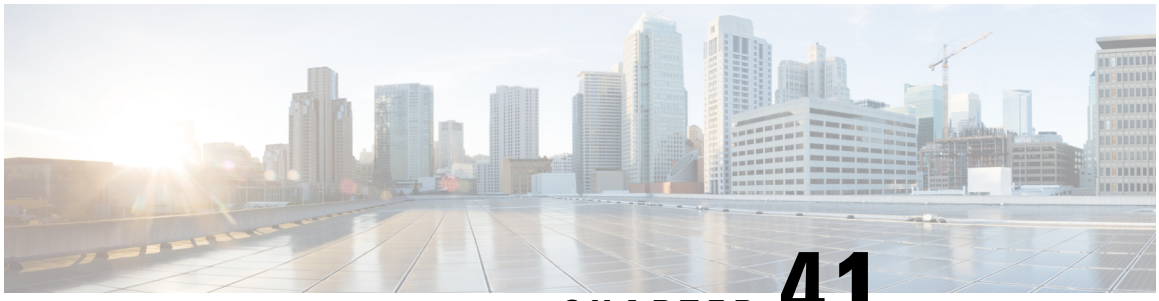
To verify that the dual radio mode is enabled, use the following **show** command:

- ```
  Device# show ap name APXXXX.4XXX.04XX config slot 1 | inc Dual
    Dual Radio Capable                              : True
    Dual Radio Mode                                 : Enabled
    Dual Radio Operation mode                       : Auto
  ```

To verify the tri-radio status, use the following **show** command:

- ```
  Device# show ap triradio status
  Tri-Radio Status : Enabled
  ```

To verify that the radio role is set, use the following **show** command:

- ```
  show ap name ap-name config slot <slot_number> | i Radio
  Radio Type                                      : 802.11ax - 5 GHz
  Radio Subband                                   : All
  Radio Role                                      : Auto
  Radio Mode                                      : Local
  Radio SubType                                   : Main
  ```
  ```



CHAPTER 40

Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard

- Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard, on page 593
- Configuring Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard Parameters (CLI), on page 594
- Verifying AP DFS Counters (CLI), on page 595
- Verifying Wi-Fi 6 Access Point Parameters, on page 596

Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard

Note We recommend you manage this feature using the Cisco Catalyst Center UI. The procedures are to be executed with for debugging purposes only.

The Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard provides a visual representation of your wireless network. The dashboard contains various dashlets which show you the Wi-Fi 6 Readiness, and the efficiency of the Wi-Fi 6 networks compared to non-Wi-Fi 6 networks. For more information, see the **Monitor Wi-Fi 6 Readiness** section in the Cisco DNA Assurance User Guide.

- **Client Distribution by Capability**: This dashlet shows all the clients associated and their capability in the wireless network. The inner circle shows the wireless protocol capabilities of all the different clients in the network. Capability here is the ability of wireless clients to associate with Wi-Fi 6 APs or non-Wi-fi 6 APs. The outer arc segment shows how many 802.11ax capable clients are joined to a Wi-Fi 6 network as well as how many of them are not.
- **Wi-Fi 6 Network Readiness**: This dashlet shows all the APs in the network. The inner circle shows the APs which are Wi-Fi 6 APs and non Wi-Fi 6 APs. The outer arc segment shows the number of Wi-Fi 6 enabled AP in the network.
- **AP Distribution by Protocol**: This dashlet shows the protocols enabled on your APs in real time.
- **Wireless Airtime Efficiency**: This dashlet compares and displays the Airtime Efficiency between your Wi-Fi 6 network and Non-Wi-Fi 6 network for each of the access categories (voice, video, best effort, background).

  The spectrum is efficiently utilized if the AP's radios can send more traffic (successful bytes transmitted to the client) in less airtime (microseconds) than other networks under similar RF conditions.

- **Wireless Latency by Client Count**: This Dashlet compares the Wireless Latency between your Wi-Fi 6 and Non-Wi-Fi 6 Network for each of the access categories (voice, video, best effort, background).

  Wireless latency is measured by the time (microseconds) it takes for a packet to be successfully transmitted from an AP to the client. Hence, AP radios with a higher client count generally have higher latency than compared to those with a lower client count under similar RF conditions.

Note **Client count** in this dashlet refers to the clients that are actively sending traffic for a given Access Category and are not just associated clients.

Configuring Cisco Catalyst Center Assurance Wi-Fi 6 Dashboard Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile pp-1`	Enables configuration for all the APs that are associated with the specified AP profile name.
Step 3	**statistics traffic-distribution** **Example:** `Device(config-ap-profile)#statistics traffic-distribution`	Enables traffic distribution feature with the specified AP profile.
Step 4	**statistics traffic-distribution interval** *interval-secs* **Example:** `Device(config-ap-profile)#statistics traffic-distribution interval 300`	Configures the interval at which the AP sends the traffic distribution statistics. Default value is 300 seconds. Valid range is between 30 and 3600 seconds. **Note** Execute this command only with the assistance from Cisco Technical Assistance Center (TAC) support engineer.
Step 5	**end** **Example:** `Device(config-ap-profile)#exit`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show wireless stats ap name** *ap-name* **traffic-distribution slot** *slot-id* **packet-count signal** {**average**| **good** | **poor**} [**last-received**] **Example:** `Device#show wireless stats ap name ff123a traffic-distribution slot 1 packet-count signal good`	Displays traffic distribution data by signal strength, if received from the AP in the latest statistics update interval. Use **last-received** keyword to view the statistics received in any statistics update interval from the AP.
Step 7	**show wireless stats ap name** *ap-name* **traffic-distribution slot** *slot-id* **airtime access-category** {**background** | **best-effort** | **video** |**voice**} [**last-received**] **Example:** `Device#show wireless stats ap name ff123a traffic-distribution slot 1 airtime access-category best-effort`	Displays the Airtime efficiency data based on access category, if received from the AP in the latest statistics update interval. Use **last-received** keyword to view the statistics received in any statistics update interval from the AP.
Step 8	**show wireless stats ap name** *ap-name* **traffic-distribution slot** *slot-id* **airtime traffic-type** {**legacy** | **mu** | **ofdma** | **su**} [**last-received**] **Example:** `Device#show wireless stats ap name ff123a traffic-distribution slot 1 traffic-type ofdma`	Displays the Airtime efficiency data based on traffic type, if received from the AP in the latest statistics update interval. Use **last-received** keyword to view the statistics received in any statistics update interval from the AP.
Step 9	**show wireless stats ap name** *ap-name* **traffic-distribution slot** *slot-id* **latency access-category** {**background** | **best-effort** | **video** | **voice**} [**last-received**] **Example:** `Device#show wireless stats ap name ff123a traffic-distribution slot 1 latency access-category best-effort`	Displays wireless latency data based on access category, if received from the AP in the latest statistics update interval. Use **last-received** keyword to view the statistics received in any statistics update interval from the AP.

Verifying AP DFS Counters (CLI)

Procedure

- To verify the DFS counter for the selected radio band, use the following command:

  show ap auto-rf dot11 {**24ghz** \| **5ghz** \| **dual-band**}]

  Example:

  `Device#show ap auto-rf dot11 dual-band`

- To verify the DFS counter for the selected radio band of a specific AP, use the following command:

show ap name *ap-name* **auto-rf dot11** {**24ghz** | **dual-band**}

Example:

```
Device#show ap name ff32a auto-rf dot11 dual-band
```

- To verify the DFS counter for the selected 5-GHz slot of a specific AP, use the following command:

  show ap name *ap-name* **auto-rf dot11 5ghz slot** *slot-id*

  Example:

```
Device#show ap name ff32a auto-rf dot11 5ghz slot 1
```

Verifying Wi-Fi 6 Access Point Parameters

Enter these commands in the AP console.

- To verify the traffic distribution statistics configuration, use the following command: **show ap traffic distribution configuration**
- To verify the exported data from the AP to the controller, use the following command: **show interfaces dot11Radio** *slot-id* **traffic distribution** {**cumulative** | **instantaneous** | **periodic**} **database**
- To verify Access Point DFS counters, use the following command: **show interfaces dot11radio** *slot-id***dfs**
- To debug the traffic distribution statistics, use the following command: {**no**} **debug traffic wireless distribution dump** {**periodic** | **aggregated**}
- To clear the traffic distribution dump, use the following command: **clear traffic distribution dump**



CHAPTER 41

Antenna Disconnection Detection

- Feature History for Antenna Disconnection Detection, on page 597
- Information About Antenna Disconnection Detection, on page 597
- Recommendations and Limitations, on page 598
- Configuring Antenna Disconnection Detection (CLI), on page 598
- Configuring Antenna Disconnection Detection (GUI), on page 599
- Detecting Broken Antenna Using SNMP Trap (CLI), on page 600
- Detecting Broken Antenna Using SNMP Trap (GUI), on page 600
- Verifying Antenna Disconnection Detection, on page 601
- Verifying Antenna Disconnection Detection (GUI), on page 602

Feature History for Antenna Disconnection Detection

This table provides release and related information for the features explained in this module.

These features are available in all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.4.1	Antenna Disconnection Detection	This feature detects the signal strength delta across the antennas on the receiver. If the delta is more than the defined limit for a specific duration, the corresponding antenna is considered to have issues.

Information About Antenna Disconnection Detection

Having multiple antennas on the transmitter and receiver of an access point (AP) results in better performance and reliability. Multiple antennas improve reception through the selection of the stronger signal or a combination of individual signals at the receiver. Therefore, detection of an impaired antenna or physical breakage of an antenna is critical to the reliability of APs.

The Antenna Disconnection Detection feature is based on the signal strength delta across the antennas on the receiver. If the delta is more than the defined limit for a specific duration, the antenna is considered to have issues.

For every detection time period that you configure, the AP sends an Inter-Access Point Protocol (IAPP) message that carries the antenna condition. This message is sent only once when the issue is detected and is displayed in the controller trap messages, SNMP traps, and controller debug logs.

Configuration Workflow

1. Configure APs.
2. Configure an AP profile.
3. Enable the feature in AP profile.
4. Configure feature parameters.
5. Verify the configuration.

Recommendations and Limitations

- The feature is supported only on the following APs:
  - Cisco Catalyst 9120AX Series Access Points
  - Cisco Catalyst 9130AX Series Access Points
  - Cisco Aironet 2800e Access Points
  - Cisco Aironet 3800e Access Points
- The SNMP trap is not supported on the Cisco Embedded Wireless Controller.
- The IAPP message is sent only when there is a change in the error condition.

Configuring Antenna Disconnection Detection (CLI)

Antenna disconnection detection works by comparing the received signal strength intensity (RSSI) of each antenna with the antenna receiving the higher RSSI. If the delta is higher than the RSSI failure threshold, the corresponding antenna is declared as broken.

The *weak-rssi* is an absolute RSSI threshold value, expressed in dBm. If the antennas detect a lower RSSI value than the one configured in *weak-rssi*, all the antennas are reported as malfunctioning. The RSSI failure threshold is evaluated only if an antenna detects a signal over the *weak-rssi* value.

Follow the procedure given below to configure antenna disconnection detection:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**antenna monitoring** **Example:** `Device(config-ap-profile)# antenna monitoring`	Enables antenna disconnection detection. To disable antenna disconnection detection, use the **no antenna monitoring** command.
Step 4	**antenna monitoring rssi-failure-threshold** *threshold-value* **Example:** `Device(config-ap-profile)# antenna monitoring rssi-failure-threshold 20`	Configures RSSI failure threshold value, in dB. Valid values range from 10 to 90, with a default of 40.
Step 5	**antenna monitoring weak-rssi** *weak-rssi-value* **Example:** `Device(config-ap-profile)# antenna monitoring weak-rssi -90`	Configures weak RSSI value, in dBm. Valid values range from -90 to -10, with a default of 60.
Step 6	**antenna monitoring detection-time** *detect-time-in-mins* **Example:** `Device(config-ap-profile)# antenna monitoring detection-time 20`	Configures the antenna disconnection detection time, in minutes. Valid values range from 9 to 180, with a default of 120.
Step 7	**end** **Example:** `Device(config-ap-profile)# end`	Saves the configuration and returns to privileged EXEC mode.

Configuring Antenna Disconnection Detection (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > AP Join**.

Step 2 In the **AP Join Profile** window, click the **General** tab.

Step 3 In the **Antenna Monitoring** check box to enable antenna monitoring.

Step 4 In the **RSSI Fail Threshold(dB)** field, enter a value, in dB. Valid values range from 10 to 90, with a default of 40.

Step 5 In the **Weak RSSI(dBm)** field, enter a value, in dBm. Valid values range from -90 to -10, with a default of 60.

Step 6 In the **Detection Time(min)** field, enter the antenna disconnection detection time, in minutes. Valid values range from 9 to 180, with a default of 120.

Step 7 Click **Update & Apply to Device**.

Detecting Broken Antenna Using SNMP Trap (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps** **Example:** `Device(config)# snmp-server enable traps`	Enables all the SNMP notification types that are available on the system.
Step 3	**trapflags ap broken-antenna** **Example:** `Device(config)# trapflags ap broken-antenna`	Enables an SNMP trap, which will be sent when an antenna fails in any Cisco AP.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Detecting Broken Antenna Using SNMP Trap (GUI)

Procedure

Step 1 Choose **Administration > Management > SNMP**.

Step 2 Click the **Wireless Traps** tab.

Step 3 Set the **Access Point** status as **Enabled**, if not done already.

Step 4 Check the **Broken Antenna** check box to enable the trap.

Step 5 Click **Apply**.

Verifying Antenna Disconnection Detection

To verify the Antenna Disconnection Detection feature configuration on an AP, use the following command:

```
Device# show ap name 3800-AP config general

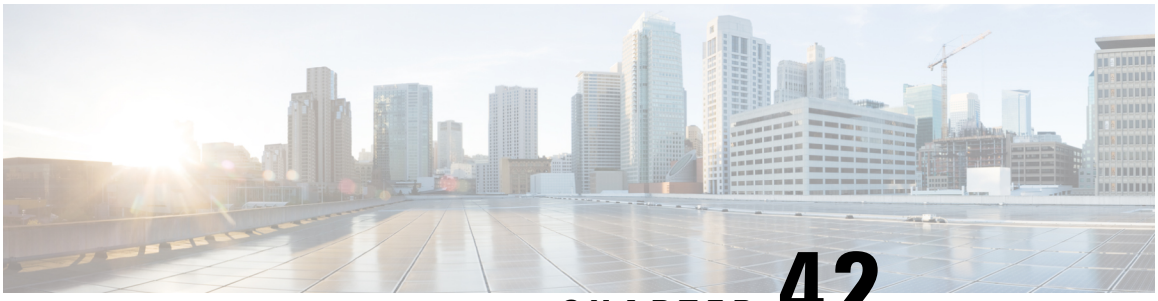
Cisco AP Name: 3800-AP
================================================

Cisco AP Identifier                             : f4db.e632.df40
Country Code                                    : Multiple Countries : US,IN,CN,CU
Regulatory Domain Allowed by Country            : 802.11bg:-ACE   802.11a:-ABCDHN
AP Country Code                                 : CN  - China
AP Regulatory Domain
  Slot 0                                        : -E
  Slot 1                                        : -C
MAC Address                                     : f4db.e62f.165a
IP Address Configuration                        : DHCP
IP Address                                      : 9.9.33.3
IP Netmask                                      : 255.255.255.0
Gateway IP Address                              : 9.9.33.1
Fallback IP Address Being Used                  :
Domain                                          :
Name Server                                     :
CAPWAP Path MTU                                 : 1485
Capwap Active Window Size                       : 1

.
.
.

AP broken antenna detection                             : Enabled
RSSI threshold                                          : 40
Weak RSSI                                               : -80
Detection Time                                          : 120

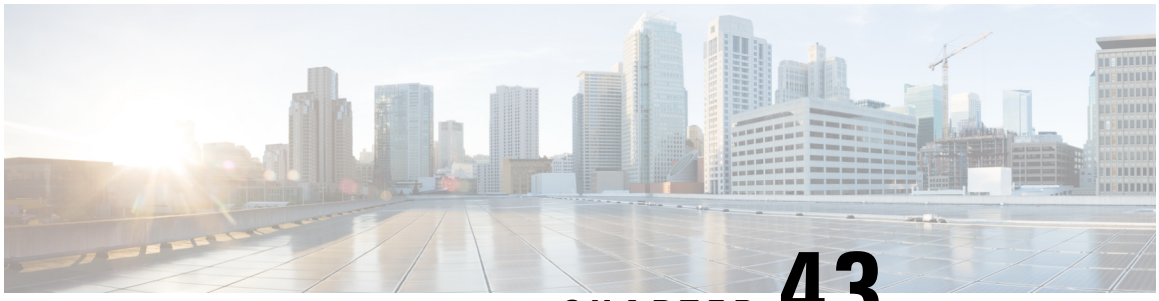
.
.
.
```

To verify the Antenna Disconnection Detection feature configuration on an AP profile, use the following command:

```
Device# show ap profile name rf-profile-24g detailed

AP Profile Name: rf-profile-24g
.
.
.
AP broken antenna detection:
  Status                                                : ENABLED
  RSSI threshold                                        : 40
  Weak RSSI                                             : -80
  Detection Time                                        : 120
```

Verifying Antenna Disconnection Detection (GUI)

Procedure

Step 1 Choose **Monitoring > Wireless > AP Statistics**.

Step 2 Click an AP name or anywhere on the row corresponding to an AP in order to activate **General** window.

Step 3 Click the **360 View** tab.

The 360 View tab is the default selection. The **Antenna Monitoring** field indicates whether the AP supports monitoring or not.



CHAPTER 42

Neighbor Discovery Protocol Mode on Access Points

- Information About Neighbor Discovery Protocol Mode, on page 603
- Configuring RRM Neighbor Discovery Mode (GUI), on page 604
- Configuring the Neighbor Discovery Protocol Mode (CLI), on page 604
- Configuring the Neighbor Discovery Protocol Type (CLI), on page 604
- Configuring Neighbor Discovery Protocol Mode in the RF Profile (GUI), on page 605
- Configuring Neighbor Discovery Protocol Mode in the RF Profile (CLI), on page 605
- Monitoring Radio Statistics-NDP Capability and NDP Mode (GUI) , on page 606
- Verifying Neighbor Discovery Protocol Mode, on page 607

Information About Neighbor Discovery Protocol Mode

In Cisco Catalyst 9124AX outdoor Access Points, the Neighbor Discovery Protocol (NDP) packets are transmitted either ON-channel on the serving radio, or OFF-channel on the RF ASIC conventional radio. The controller has a knob to select the NDP mode for Cisco Catalyst 9124AX outdoor APs based on the deployment requirements. In Cisco IOS XE Bengaluru 17.5.1, Cisco Catalyst 9124AX outdoor APs support both ON-Channel and OFF-Channel NDP mode.

The Cisco Catalyst 9124AX outdoor AP advertises the following NDP mode capabilities while joining the controller:

- ON-Channel (Serving channel)
- OFF-Channel (RF ASIC radio)
- Both (Serving channel and RF ASIC radio)

The supported values for NDP mode are AUTO and OFF-Channel. By default, the NDP mode is set to AUTO.

If the configured NDP mode is AUTO, the AP determines which NDP mode is to be used. The Cisco Catalyst 9124AX outdoor AP uses ON-Channel when the controller is configured for AUTO NDP mode. If the NDP mode that is configured is OFF-Channel, the AP uses OFF-Channel for NDP mode.

Use Cases

You must configure the controller NDP mode to OFF-channel in order to support brownfield deployment. A brownfield deployment refers to the mixed deployment of Cisco Catalyst 9124AX with other APs that do not

support RF ASIC conventional radio. APs that support RF ASIC conventional radio are Cisco Catalyst 9120 Series Access Points, Cisco Catalyst 9130 Series Access Points, and Cisco Catalyst 9124 Series Access Points.

Configuring RRM Neighbor Discovery Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.

Step 2 In the **Radio Resource Management** window, click either the **5 GHz Band** or the **2.4 GHz Band** tab.

Step 3 In the **General** tab, under the **Noise/Interference/Rogue/CleanAir/SI Monitoring Channels** section, click the **RRM Neighbor Discovery Mode** toggle button to configure either of the following modes:

- **AUTO**: If the NDP mode that is configured is **AUTO**, the controller selects ON-Channel as the NDP mode. (The default is set as AUTO).
- **OFF-CHANNEL**: If the NDP mode configured is **OFF-CHANNEL**, the controller selects **OFF-CHANNEL** as the NDP mode.

Step 4 Click **Apply**.

Configuring the Neighbor Discovery Protocol Mode (CLI)

To configure the NDP mode for an AP, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rrm ndp-mode** {**auto** | **off-channel**} **Example:** `Device(config)# ap dot11 24ghz rrm ndp-mode off-channel`	Configures the operating mode for 802.11a neighbor discovery. The **Off-channel** command enables NDP packets on the RF ASIC radio and the **auto** command enables the auto mode.

Configuring the Neighbor Discovery Protocol Type (CLI)

To configure the NDP type for an AP , follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm ndp-type** {**protected** | **transparent**} **Example:** `Device(config)# ap dot11 6ghz rrm ndp-type`	Configures the NDP type for 802.11a, 802.11b, or 802.11 6-GHz neighbor discovery. The two types are protected and transparent.

Configuring Neighbor Discovery Protocol Mode in the RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 Click **Add**.
The **Add RF Profile** window is displayed.

Step 3 Click the **General** tab.

Step 4 Click the **NDP Mode** toggle button to select the NDP mode as **AUTO** or as **OFF-CHANNEL**.

Step 5 Click **Apply to Device**.

Configuring Neighbor Discovery Protocol Mode in the RF Profile (CLI)

To configure the NDP mode for an AP under the RF profile, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rf-profile** *rf-profile-name*	Enters the RF profile configuration.

	Command or Action	Purpose
	Example: `Device(config)# ap dot11 24ghz rf-profile rf-profile-name`	
Step 3	**ndp-mode** {**auto** | **off-channel**} **Example:** `Device(config-rf-profile)# ndp-mode off-channel`	Configures the operating mode for neighbor discovery. **Off-channel** enables NDP packets on the RF ASIC radio and **auto** enables the auto mode.

Monitoring Radio Statistics-NDP Capability and NDP Mode (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **Radio Statistics**.

Step 2 Click either **5 GHz Radios**, **2.4 GHz Radios**, or **Dual-Band Radios** tab.
The corresponding radio band window displays the list of configured APs.

Step 3 To view the general attributes of an AP, click the corresponding AP to display the **General** tab. The following information is displayed:

- **AP Name**: Displays the assigned identifier for the AP, which is unique within the network. The AP name can be ASCII characters from 32 to 126, without leading and trailing spaces.
- **IP Address**: Displays the IP address assigned to the AP in dotted-decimal format.
- **AP Mode**: Displays the configured AP mode. The supported modes are:
  - **Local**: It is the default mode, and it offers a basic service set (BSS) on a specific channel. When the AP does not transmit wireless client frame, it scans other channels to measure noise interference, discover rogue devices, and check for matches against Intrusion Detection System (IDS) events.
  - **Monitor**: An AP in monitor mode does not transmit. It is a dedicated sensor that checks IDS events, detects rogue APs, and determines the position of wireless stations.
  - **Sniffer**: The controller enables you to configure an AP as a network *sniffer*, which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on. Sniffers allow you to monitor and record network activity and detect problems.
  - **Bridge**: The AP becomes a dedicated point-to-point or point-to multipoint bridge. Two APs in bridge mode can connect two remote sites. Multiple APs can also form an indoor or outdoor mesh. Note that you cannot connect to the bridge with clients.
  - **Clear**: Returns the AP back to client-serving mode depending on the remote site tag configuration.
- **MAC Address**: Displays the registered MAC address on the controller.
- **Number of Slots** : Displays the number of slots supported by the AP.

- **Radio Type**: Displays the radio band configured on the controller. By default, both, 802.11b/g/n (2.4-GHz) and 802.11a/n/ac (5-GHz) bands are enabled.
- **Slot ID**: Displays the slot on which radio is installed.
- **Sub band Type**: Displays the configured radio sub-band.
- **NDP Capability**: Displays the supported Neighbor Discovery Protocol (NDP) capability. The AP advertises the following NDP mode capabilities while joining the controller:
  - ON-Channel (Serving channel)
  - OFF-Channel (RHL radio)
  - Both (Serving channel and RHL radio)

  Note Only Cisco Catalyst 9124AX outdoor Access Points support both ON-channel and OFF-channel NDP capability from Cisco IOS XE Bengaluru 17.5.1.

- **NDP Mode**: Displays the configured NDP mode. If the NDP mode that is configured is AUTO, the controller selects ON-Channel as the NDP mode. If the NDP-mode that is configured is OFF-Channel, the controller selects OFF-Channel as the NDP mode.

Verifying Neighbor Discovery Protocol Mode

To verify the NDP mode, run the following commands:

```
Device# show ap rf-profile name test-24g
Description                     : test
RF Profile Name                 : test-24g
Band                            : 2.4 GHz
Transmit Power Threshold v1     : -70 dBm
Min Transmit Power              : -10 dBm
Max Transmit Power              : 30 dBm
.
.
.
NDP mode                        : Auto
.
.
.

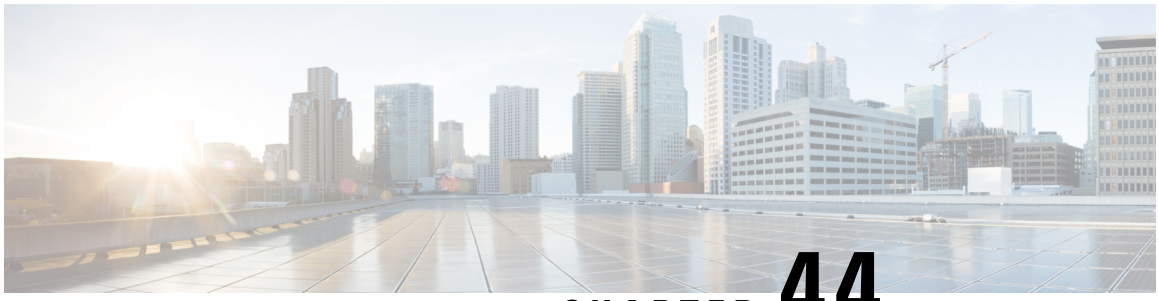
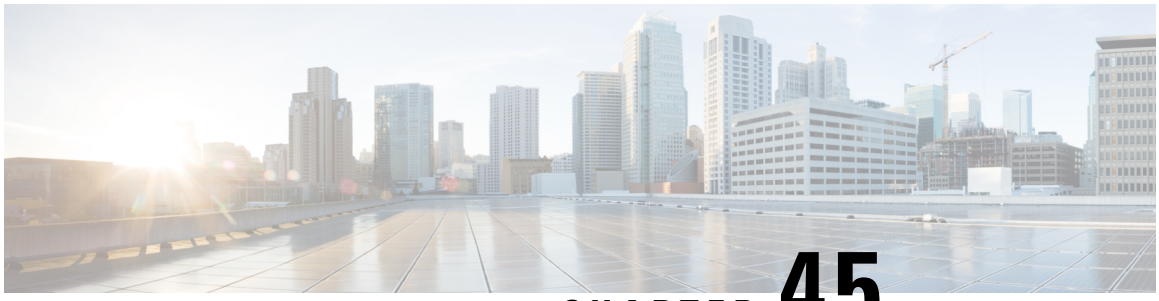
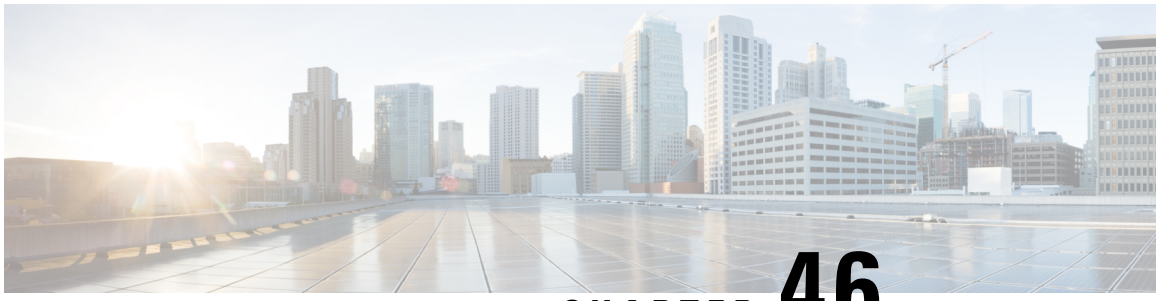
Device# show ap rf-profile name test-5g detail
Description                     : Test
RF Profile Name                 : test-5g
Band                            : 5 GHz
Transmit Power Threshold v1     : -70 dBm
Min Transmit Power              : -10 dBm
Max Transmit Power              : 30 dBm
.
.
.
NDP mode                        : Off-channel
.
.
.
```

```
Device# show ap name ap-name config dot11 24ghz
Cisco AP Identifier                             : 3cxx.0exx.36xx
Cisco AP Name                                   : Cisco-9105AXW-AP
Country Code                                    : Multiple Countries: US,MK,J4,IN
Regulatory Domain Allowed by Country            : 802.11bg:-AEJPQU   802.11a:-ABDEIJNPQU
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -A
MAC Address                                     : 5cxx.0dxx.e0xx
IP Address Configuration                        : DHCP
.
.
.
NDP mode                                        :  Off-channel
.
.
.

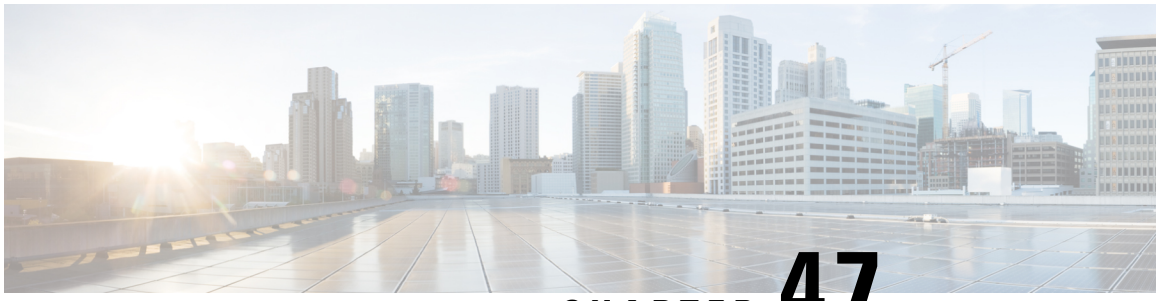
Device# show ap name ap-name config dot11 5ghz
Cisco AP Identifier                             : 3cxx.0exx.36xx
Cisco AP Name                                   : Cisco-9105AXW-AP
Country Code                                    : Multiple Countries: US,MK,J4,IN
Regulatory Domain Allowed by Country            : 802.11bg:-AEJPQU   802.11a:-ABDEIJNPQU
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -B
MAC Address                                     : 5cxx.0dxx.e0xx
IP Address Configuration                        : DHCP
IP Address                                      : Disabled
.
.
.
NDP mode                                        :  On-channel
.
.
.

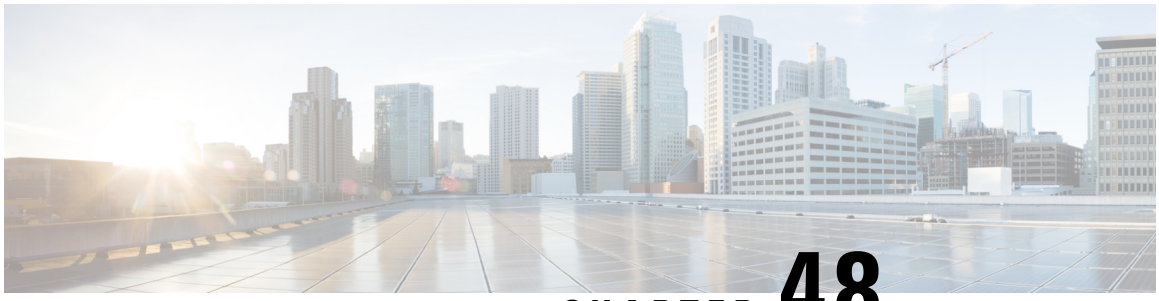
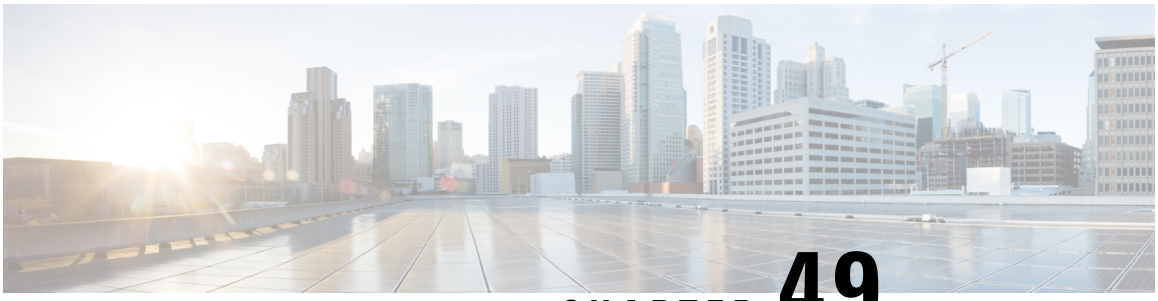
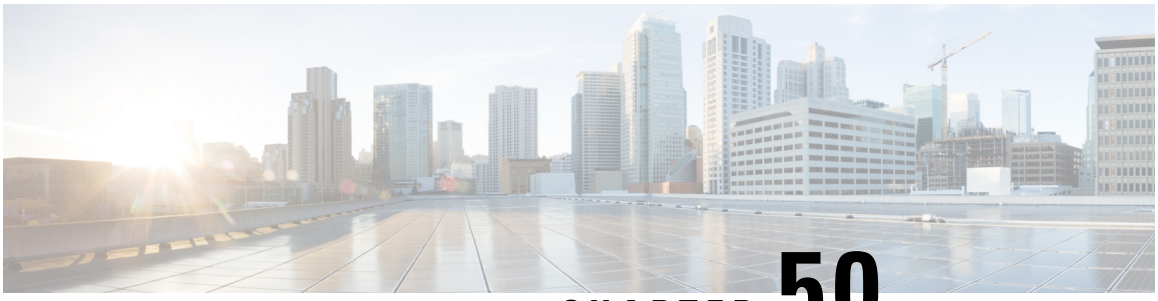
Device# show ap dot11 24ghz monitor
Default 802.11b AP monitoring
  802.11b Monitor Mode                  : Enabled
  802.11b Monitor Channels              : Country channels
  802.11b RRM Neighbor Discover Type    : Transparent
  802.11b AP Coverage Interval          : 180 seconds
  802.11b AP Load Interval              : 60 seconds
  802.11b AP Measurement Interval       : 180 seconds
  802.11b AP Reporting Interval         : 180 seconds
  802.11b NDP RSSI Normalization        : Enabled
  802.11b Neighbor Timeout factor       : 20
  802.11b NDP mode                      : Auto

Device# show ap dot11 5ghz monitor
Default 802.11a AP monitoring
  802.11a Monitor Mode                  : Enabled
  802.11a Monitor Channels              : Country channels
  802.11a RRM Neighbor Discover Type    : Transparent
  802.11a AP Coverage Interval          : 180 seconds
  802.11a AP Load Interval              : 60 seconds
  802.11a AP Measurement Interval       : 180 seconds
  802.11a AP Reporting Interval         : 180 seconds
  802.11a NDP RSSI Normalization        : Enabled
  802.11a Neighbor Timeout factor       : 20
  802.11a NDP mode                      : Auto
```



CHAPTER 43

6-GHz Band Operations

The following topics describe the features that are specific to 6-GHz band radio:

- Configuring Preferred Scanning Channels in the RF Profile (GUI), on page 609
- Configuring Preferred Scanning Channels in the RF Profile (CLI), on page 610
- Configuring Broadcast Probe Response in RF Profile (GUI), on page 610
- Configuring Broadcast Probe Response in RF Profile (CLI), on page 610
- Configuring FILS Discovery Frames in the RF Profile (GUI), on page 611
- Configuring FILS Discovery Frames in the RF Profile (CLI), on page 612
- Configuring Multi BSSID Profile (GUI), on page 612
- Configuring Multi BSSID Profile, on page 613
- Configuring Multi-BSSID in the RF Profile (GUI), on page 613
- Configuring Multi-BSSID in the RF Profile (CLI), on page 614
- Configuring Dynamic Channel Assignment Freeze (CLI), on page 614
- Information About 6-GHz Client Steering, on page 615

Configuring Preferred Scanning Channels in the RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

Step 2 In the **RF** tab, click **Add**.
The **Add RF Profile** page is displayed.

Step 3 Choose the **RRM** tab.

Step 4 Choose the **DCA** tab.

Step 5 In the **Dynamic Channel Assignment** section, select the required channels in **DCA Channels** section.

Step 6 In the **PSC Bias** field, click the toggle button to enable the preferred scanning channel bias for DCA.

Step 7 Click **Apply to Device**.

Configuring Preferred Scanning Channels in the RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 6ghz rf-profile** *rf-profile-name* **Example:** `Device(config)# ap dot11 6ghz rf-profile rf-profile-name`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**channel psc** **Example:** `Device(config-rf-profile)# channel psc`	Configures the RF Profile DCA settings and enables the preferred scanning channel bias for DCA.

Configuring Broadcast Probe Response in RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

Step 2 In the **RF** tab, click **Add**.
The **Add RF Profile** page is displayed.

Step 3 Choose the **802.11ax** tab.

Step 4 In the **6 GHz Discovery Frames** section, click the **Broadcast Probe Response** option.

Step 5 In the **Broadcast Probe Response Interval** field, enter the broadcast probe response time interval in milli-seconds (ms). The value range is between 5 ms and 25 ms. The default value is 20 ms.

Step 6 Click **Apply to Device**.

Configuring Broadcast Probe Response in RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**ap dot11 6ghz rf-profile** *rf-profile-name* **Example:** `Device(config)# ap dot11 6ghz rf-profile rf-profile-name`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**dot11ax bcast-probe-response** **Example:** `Device(config-rf-profile)# dot11ax bcast-probe-response`	Configures broadcast probe response.
Step 4	**dot11ax bcast-probe-response time-interval** *time-interval* **Example:** `Device(config-rf-profile)# dot11ax bcast-probe-response time-interval 20`	Configures broadcast probe response interval.

Configuring FILS Discovery Frames in the RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

Step 2 In the **RF** tab, click **Add**.
The **Add RF Profile** page is displayed.

Step 3 Choose the **802.11ax** tab.

Step 4 In the **6 GHz Discovery Frames** section, click the **FILS Discovery** option.

Note To prevent the transmission of discovery FILS frames when the discovery frames are set to **None** in the RF profile, ensure that you disable FILS discovery frames by either switching to the 5-GHz or the 2.4-GHz bands on the AP or by selecting the Broadcast Probe Response option.

Step 5 Click **Apply to Device**.

Configuring FILS Discovery Frames in the RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 6ghz rf-profile** *rf-profile-name* **Example:** `Device(config)# ap dot11 6ghz rf-profile rf-profile-name`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**dot11ax fils-discovery** **Example:** `Device(config-rf-profile)# dot11ax fils-discovery`	Configures the 802.11ax FILS discovery. **Note** To prevent the transmission of discovery FILS frames when the discovery frames are set to None in the RF profile, ensure that you disable FILS discovery frames by either switching to the 5-GHz or the 2.4-GHz bands on the AP or by changing to Broadcast Probe Response.

Configuring Multi BSSID Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Multi BSSID**.

Step 2 Click **Add**.
The **Add Multi BSSID Profile** page is displayed.

Step 3 Enter the name and the description of the BSSID profile.

Step 4 Enter the following 802.11ax parameters:

a) **Downlink OFDMA**
b) **Uplink OFDMA**
c) **Downlink MU-MIMO**
d) **Uplink MU-MIMO**
e) **Target Waketime**
f) **TWT Broadcast Support**

Step 5 Click **Apply to Device**.

Configuring Multi BSSID Profile

To configure the multi BSSID profile for 6-Ghz band radio, follow the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile multi-bssid** *multi-bssid-profile-name* **Example:** `Device (config)# wireless profile multi-bssid multi-bssid-profile-name`	Configures the multi BSSID profile. Enters the multi BSSID profile configuration.
Step 3	**dot11ax** {**downlink-mumimo** | **downlink-ofdma** | **target-waketime** | **twt-broadcast** | **uplink-mumimo** | **uplink-ofdma**} **Example:** `Device (config-wireless-multi-bssid-profile)# dot11ax downlink-mumimo`	Configures the 802.11ax parameters.

Configuring Multi-BSSID in the RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

Step 2 In the **RF** tab, click **Add**.
The **Add RF Profile** page is displayed.

Step 3 Choose the **802.11ax** tab.

Step 4 In the **Multi BSSID Profile** field, choose the profile from the drop-down list.

Step 5 Click **Apply to Device**.

Configuring Multi-BSSID in the RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 6ghz rf-profile** *rf-profile-name* **Example:** `Device(config)# ap dot11 6ghz rf-profile rf-profile-name`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**dot11ax multi-bssid-profile** *multi-bssid-profile-name* **Example:** `Device(config-rf-profile)# dot11ax multi-bssid-profile multi-bssid-profile-name`	Configures 802.11ax multi BSSID profile name, in the RF profile configuration mode.

Configuring Dynamic Channel Assignment Freeze (CLI)

When the 6-GHz radios receive the right channels, disable DCA for 6-GHz by issuing the following command:

Before you begin

Ensure that Dynamic Channel Assignment (DCA) for 6-GHz is enabled. Wait for the 6-GHz radios to get stabilized with the right set of channel assignments.

Procedure

	Command or Action	Purpose
Step 1	**no ap dot11 6ghz rrm channel dca global auto** **Example:** `Device# no ap dot11 6ghz rrm channel dca global auto`	Disables DCA for 6-GHz bands.

Information About 6-GHz Client Steering

The 6-GHz band provides more channels, more bandwidth, and has less network congestion when compared to the existing 2.4-GHz and 5-GHz bands. As a result, wireless clients that are 6-GHz capable connect to the 6-GHz radio to take advantage of these benefits.

This topic provides details about 6-GHz client steering for APs supporting 6-GHz band.

The 6-GHz client steering takes place when the controller receives a periodic client statistics report from the 2.4-GHz band or the 5-GHz band. The client steering configuration is enabled under WLAN, and is configured only for clients that are 6-GHz capable. If a client in the report is 6-GHz capable, then client steering is triggered, and the client is steered to the 6-GHz band.

Configuring 6-GHz Client Steering in the Global Configuration Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

Step 2 Click the **6 GHz Client Steering** tab. Client steering is configurable per WLAN.

Step 3 In the **6 GHz Transition Minimum Client Count** field, enter a value to set the minimum number of clients for client steering. The default value is three clients. The value range is between 0 and 200 clients.

Step 4 In the **6 GHz Transition Minimum Window Size** field, enter a value to set the minimum window size of client steering. The default value is three clients. The value range is between 0 and 200 clients.

Step 5 In the **6 GHz Transition Maximum Utilization Difference** field, enter a value to set the maximum utilization difference for steering. The value range is between 0 percent to 100 percent. The default value is 20.

Step 6 In the **6 GHz Transition Minimum 2.4 GHz RSSI Threshold** field, enter a value to set the minimum value for client steering 2.4-GHz RSSI threshold.

Step 7 In the **6 GHz Transition Minimum 5 GHz RSSI Threshold** field, enter a value to set the minimum value for client steering 5-GHz RSSI threshold.

Step 8 Click **Apply**.

Configuring 6-GHz Client Steering in the Global Configuration Mode

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless client client-steering client-count** *min-num-clients* **Example:** `Device(config)# client-steering client-count 3`	Sets the minimum number of clients for client steering. The value range is between 0 and 200.
Step 3	**wireless client client-steering window-size** *window-size* **Example:** `Device(config)# client-steering window-size 5`	Sets the minimum window size of client steering. The value range is between 0 and 200.
Step 4	**wireless client client-steering util-threshold** *threshold* **Example:** `Device(config)# wireless client client-steering util-threshold 25`	Sets the maximum channel utilization difference (2.4-GHz or 5-GHz to 6-GHz) for steering. The value range is between 0 to 100 percent.
Step 5	**wireless client client-steering min-rssi-24ghz -70** **Example:** `Device(config)# wireless client client-steering min-rssi-24ghz -70`	Sets the minimum value for client steering the 2.4-GHz RSSI threshold.
Step 6	**wireless client client-steering min-rssi-5ghz -75** **Example:** `Device(config)# wireless client client-steering min-rssi-5ghz -75`	Sets the minimum value for client steering the 5-GHz RSSI threshold.

Configuring 6-GHz Client Steering on the WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.
The **Add WLAN** page is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Check the **6 GHz Client Steering** check box to enable client steering on the WLAN.

Step 5 Click **Apply to Device**.

Configuring 6-GHz Client Steering on the WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-name 18 ssid-name`	Enters WLAN configuration submode.
Step 3	**client-steering** **Example:** `Device(config-wlan)# client-steering`	Configures 6-GHz client steering on the WLAN.

Verifying 6-GHz Client Steering

To verify client steering, run the following commands:

```
Device# show wlan wlan-id
WLAN Profile Name     : wlan1
================================================
Identifier                                : 1
Description                               :
Network Name (SSID)                       : ssid-demo
Status                                    : Disabled
Broadcast SSID                            : Enabled
.
.
.
6Ghz Client Steering                      : Enabled
.
.
.

Device# show wireless client steering
Client Steering Configuration Information
  Macro to micro transition threshold                 : -55 dBm
  Micro to Macro transition threshold                 : -65 dBm
  Micro-Macro transition minimum client count         : 3
  Micro-Macro transition client balancing window      : 3
  Probe suppression mode                              : Disabled
  Probe suppression transition aggressiveness         : 3
  Probe suppression hysteresis                        : -6 dB
  6Ghz transition minimum client count                : 3
  6Ghz transition minimum window size                 : 3
  6Ghz transition maximum channel util difference     : 20%
  6Ghz transition minimum 2.4Ghz RSSI threshold       : -60 dBm
  6Ghz transition minimum 5Ghz RSSI threshold         : -65 dBm

WLAN Configuration Information
```

```
WLAN Profile Name                    11k Neighbor Report       11v BSS Transition
-----------------------------------------------------------------------------------------
12   test1                           Enabled                   Enabled
8    test                            Enabled                   Enabled
```

PART V

Network Management

- AP Packet Capture, on page 621
- DHCP Option82, on page 625
- RADIUS Realm, on page 637
- RADIUS Accounting, on page 643
- RADIUS Call Station Identifier, on page 649
- RADIUS VSA, on page 651
- Cisco StadiumVision, on page 657
- Persistent SSID Broadcast, on page 661
- Network Monitoring, on page 663
- Creating a Lobby Ambassador Account, on page 667
- Lobby Ambassador Account, on page 671
- Guest User Accounts, on page 679
- Link Local Bridging, on page 683
- Web Admin Settings, on page 687
- Web UI Configuration Command Accounting in TACACS Server, on page 693



CHAPTER 44

AP Packet Capture

- Introduction to AP Client Packet Capture, on page 621
- Enabling Packet Capture (GUI), on page 621
- Enabling Packet Capture (CLI), on page 622
- Create AP Packet Capture Profile and Map to an AP Join Profile (GUI), on page 622
- Create AP Packet Capture Profile and Map to an AP Join Profile, on page 623
- Start or Stop Packet Capture, on page 623

Introduction to AP Client Packet Capture

The AP Client Packet Capture feature allows the packets on an AP to be captured for wireless client troubleshooting. The packet capture operation is performed on the AP by the radio drivers on the current channel on which it is operational, based on the specified packet capture filter. All the packets that are captured for a specific client are uploaded to a file in the FTP server. This file can be opened in Wireshark for packet inspection.

Limitations for AP Client Packet Capture

- The packet capture task can be performed for only one client at a time per site.
- Packet capture can be started on a specific AP or a set of APs using static mode. It can be started or stopped for the same client on different APs, when the capture is in progress.

  When packet capture is started in auto mode, system automatically selects the set of nearby APs to start packet capture for a specific client. In this mode, you cannot start or stop packet capture on individual APs. Use the **stop all** command to stop the packet capture when it is started in auto-mode.
- After the SSO is complete, the packet capture action will not continue after a switchover.

Enabling Packet Capture (GUI)

Procedure

Step 1 Choose **Troubleshooting** > **AP Packet Capture**.

Step 2 On the **Troubleshooting** page, in the **Start Packet Capture** section, in the **Client MAC Address** field, enter the client's MAC address. Enter the MAC address either in *xx:xx:xx:xx:xx:xx*, *xx-xx-xx-xx-xx-xx*, or *xxxx.xxxx.xxxx* format.

Step 3 From the **Capture Mode** options, choose **Auto**.

Step 4 Click **Start**.

Enabling Packet Capture (CLI)

Follow the procedure given below to enable packet capture:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap packet-capture start** *client-mac-address* **auto** **Example:** `Device# ap packet-capture start 0011.0011.0011 auto`	Enables packet capture for the specified client on a set of nearby access points.

Create AP Packet Capture Profile and Map to an AP Join Profile (GUI)

Procedure

Step 1 Click **Configuration** > **Tags & Profiles** > **AP Join Profile**.

Step 2 Click **Add** to create a new AP Join Profile and enter the requisite details.

Step 3 In the **Add AP Join Profile** area, click **AP** > **Packet Capture**.

Step 4 Click the **Plus** icon to create a new Packet Capture profile or select one from the drop-down menu.

Step 5 Click **Save**.

Create AP Packet Capture Profile and Map to an AP Join Profile

While packet capture profile configurations are used for an AP, the packet capture profile is mapped to an AP profile. The AP profile is in turn mapped to site tag.

While starting packet capture, APs use the packet capture profile configurations based on the site and AP join profile they belong to.

Follow the procedure given below to create an AP packet capture profile and map it to an AP join profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode..
Step 2	**wireless profile ap packet-capture** *packet-capture-profile-name* **Example:** `Device(config)# wireless profile ap packet-capture test1`	Configures an AP profile.
Step 3	**ap profile** *profile-name* **Example:** `Device(config)# ap profile default-ap-profile`	Configures an AP packet capture profile.
Step 4	**packet-capture** *profile-name* **Example:** `Device(config-ap-profile)# packet-capture capture-test`	Enables packet capture on the AP profile.
Step 5	**end** **Example:** `Device(config-ap-profile)# end`	Exits the AP profile configuration mode.
Step 6	**show wireless profile ap packet-capture detailed** *profile-name* **Example:** `Device# show wireless profile ap packet-capture detailed test1`	Displays detailed information of the selected AP packet capture profile.

Start or Stop Packet Capture

Perform either of these tasks to start or stop a packet capture procedure.

Procedure

	Command or Action	Purpose
Step 1	**ap packet-capture start** *client-mac-address* {**auto** | **static** *ap-name* } **Example:** `Device# ap packet-capture start 0011.0011.0011 auto`	Enables packet capture for a client.
Step 2	**ap packet-capture stop** *client-mac-address* {**all** | **static** *ap-name* } **Example:** `Device# ap packet-capture stop 0011.0011.0011 all`	Disables packet capture for a client.



CHAPTER 45

DHCP Option82

- Information About DHCP Option 82, on page 625
- Configuring DHCP Option 82 Global Interface, on page 627
- Configuring DHCP Option 82 Format, on page 629
- Configuring DHCP Option82 Through a VLAN Interface, on page 630

Information About DHCP Option 82

DHCP Option 82 is organized as a single DHCP option that contains information known by the relay agent. This feature provides additional security when DHCP is used to allocate network addresses, and enables the Cisco controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.

The controller can be configured to add Option 82 information to DHCP requests from clients before forwarding the requests to a DHCP server. The DHCP server can then be configured to allocate IP addresses to the wireless client based on the information present in DHCP Option 82.

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the Options field of the DHCP message. The data items themselves are also called options. Option 82 contains information known by the relay agent.

The Relay Agent Information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. Option 82 was designed to allow a DHCP Relay Agent to insert circuit−specific information into a request that is being forwarded to a DHCP server. This option works by setting two suboptions:

- Circuit ID
- Remote ID

The Circuit ID suboption includes information that is specific to the circuit the request came in on. This suboption is an identifier that is specific to the relay agent. Thus, the circuit that is described will vary depending on the relay agent.

The Remote ID suboption includes information on the remote host–end of the circuit. This suboption usually contains information that identifies the relay agent. In a wireless network, this would likely be a unique identifier of the wireless access point.

Note All valid Remote ID combinations are separated with a colon (:) as the delimiter.

You can configure the following DHCP Option 82 options in a controller :

- DHCP Enable
- DHCP Opt82 Enable
- DHCP Opt82 Ascii
- DHCP Opt82 RID
- DHCP Opt Format
- DHCP AP MAC
- DHCP SSID
- DHCP AP ETH MAC
- DHCP AP NAME
- DHCP Site Tag
- DHCP AP Location
- DHCP VLAN ID

Note The controller includes the SSID in ASCII and the VLAN-ID in hexadecimal format within the remote-ID sub-option of option 82 in the outgoing DHCP packets to the server for the following configurations:

```
ipv4 dhcp opt82 format ssid
ipv4 dhcp opt82 format vlan-id
```

However, if *ipv4 dhcp opt82 ascii* configuration is also present, the controller adds VLAN-ID and SSID in ASCII format.

For Cisco Catalyst 9800 Series Configuration Best Practices, see the following link: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html

Configuring DHCP Option 82 Global Interface

Configuring DHCP Option 82 Globally Through Server Override (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp-relay information option server-override** **Example:** `Device(config)# ip dhcp-relay information option server-override`	Inserts global server override and link selection suboptions.

Configuring DHCP Option 82 Through Server Override (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp compatibility suboption server-override** [**cisco** | **standard**] **Example:** `Device(config)# ip dhcp compatibility suboption server-override cisco`	Configures the server override suboption to an RFC or Cisco specific value.
Step 3	**ip dhcp compatibility suboption link-selection** [**cisco** | **standard**] **Example:** `Device(config)# ip dhcp compatibility suboption link-selection cisco`	Configures the link-selection suboption to an RFC or Cisco specific value.

Configuring DHCP Option 82 Globally Through Different SVIs (GUI)

Procedure

Step 1 Choose **Configuration > VLAN**.

Step 2 Choose a VLAN from the drop-down list.

The **Edit SVI** window appears.

Step 3 Click the **Advanced** tab.

Step 4 Choose an option from the **IPv4 Inbound ACL** drop-down list.

Step 5 Choose an option from the **IPv4 Outbound ACL** drop-down list.

Step 6 Choose an option from the **IPv6 Inbound ACL** drop-down list.

Step 7 Choose an option from the **IPv6 Outbound ACL** drop-down list.

Step 8 Enter an IP address in the **IPv4 Helper Address** field.

Step 9 Set the status to **Enabled** if you want to enable the **Relay Information Option** setting.

Step 10 Enter the **Subscriber ID**.

Step 11 Set the status to **Enabled** if you want to enable the **Server ID Override** setting.

Step 12 Set the status to **Enabled** if you want to enable the **Option Insert** setting.

Step 13 Choose an option from the **Source-Interface Vlan** drop-down list.

Step 14 Click **Update & Apply to Device**.

Configuring DHCP Option 82 Globally Through Different SVIs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp-relay source-interface vlan** *vlan-id* **Example:** `Device(config)# ip dhcp-relay source-interface vlan 74`	Sets global source interface for relayed messages.

Configuring DHCP Option 82 Format

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy pp3`	Enables configuration for the specified profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Shuts down the profile policy.
Step 4	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 72`	Assigns the profile policy to a VLAN.
Step 5	**session-timeout** *value-btwn-20-86400* **Example:** `Device(config-wireless-policy)# session-timeout 300`	(Optional) Sets the session timeout value in seconds. The range is between 20-86400.
Step 6	**idle-timeout** *value-btwn-15-100000* **Example:** `Device(config-wireless-policy)# idle-timeout 15`	(Optional) Sets the idle timeout value in seconds. The range is between 15-100000.
Step 7	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Enables central switching.
Step 8	**ipv4 dhcp opt82** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82`	Enables DHCP Option 82 for the wireless clients.
Step 9	**ipv4 dhcp opt82 ascii** **Example:**	(Optional) Enables ASCII on the DHCP Option 82 feature.

	Command or Action	Purpose
	`Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	
Step 10	**ipv4 dhcp opt82 rid** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	(Optional) Supports the addition of Cisco 2 byte Remote ID (RID) for the DHCP Option 82 feature.
Step 11	**ipv4 dhcp opt82 format** {**ap_ethmac**|**ap_location**|**apmac**|**apname**|**policy_tag**|**ssid**|**vlan_id**} **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 format apmac`	Enables DHCP Option 82 on the corresponding AP. For information on the various options available with the command, see Cisco Catalyst 9800 Series Wireless Controller Command Reference.
Step 12	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Configuring DHCP Option82 Through a VLAN Interface

Configuring DHCP Option 82 Through Option-Insert Command (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 3	**ip dhcp relay information option-insert** **Example:** `Device(config-if)# ip dhcp relay information option-insert`	Inserts relay information in BOOTREQUEST.
Step 4	**ip address** *ip-address* **Example:**	Configures the IP address for the interface.

	Command or Action	Purpose
	`Device(config-if)# ip address 9.3.72.38 255.255.255.0`	
Step 5	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configures the destination address for UDP broadcasts.
Step 6	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the MOP for an interface.
Step 7	**[no] mop sysid** **Example:** `Device(config-apgroup)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.

Configuring DHCP Option 82 Through the server-ID-override Command (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp compatibility suboption server-override cisco** **Example:** `Device(config)# ip dhcp compatibility suboption server-override cisco`	Configures the server-id override suboption to an RFC or Cisco specific value.
Step 3	**ip dhcp compatibility suboption link-selection cisco** **Example:** `Device(config)# ip dhcp compatibility suboption link-selection cisco`	Configures the link-selection suboption to an RFC or Cisco specific value.
Step 4	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 5	**ip dhcp relay information option server-id-override** **Example:**	Inserts the server id override and link selection suboptions.

	Command or Action	Purpose
	`Device(config-if)# ip dhcp relay information option server-id-override`	
Step 6	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	Configures the IP address for the interface.
Step 7	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configures the destination address for UDP broadcasts.
Step 8	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables MOP for an interface.
Step 9	**[no] mop sysid** **Example:** `Device(config-if)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.

Configuring DHCP Option 82 Through a Subscriber-ID (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 3	**ip dhcp relay information option subscriber-id** *subscriber-id* **Example:** `Device(config-if)# ip dhcp relay information option subscriber-id test10`	Inserts the subscriber identifier suboption.
Step 4	**ip address** *ip-address* **Example:**	Configures the IP address for the interface.

	Command or Action	Purpose
	`Device(config-if)# ip address 9.3.72.38 255.255.255.0`	
Step 5	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configures the destination address for UDP broadcasts.
Step 6	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables MOP for an interface.
Step 7	**[no] mop sysid** **Example:** `Device(config-apgroup)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.

Configuring DHCP Option 82 Through server-ID-override and subscriber-ID Commands (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 3	**ip dhcp relay information option server-id-override** **Example:** `Device(config-if)# ip dhcp relay information option server-id-override`	Inserts server ID override and link selection suboptions.
Step 4	**ip dhcp relay information option subscriber-id** *subscriber-id* **Example:** `Device(config-if)# ip dhcp relay information option subscriber-id test10`	Inserts the subscriber identifier suboption.

	Command or Action	Purpose
Step 5	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	Configures the IP address for the interface.
Step 6	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configures the destination address for UDP broadcasts.
Step 7	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the MOP for an interface.
Step 8	**[no] mop sysid** **Example:** `Device(config-apgroup)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.

Configuring DHCP Option 82 Through Different SVIs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 72`	Configures a VLAN ID.
Step 3	**ip dhcp relay source-interface vlan** *vlan-id* **Example:** `Device(config-if)# ip dhcp relay source-interface vlan 74`	Configures a source interface for relayed messages on a VLAN ID.
Step 4	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	Configures the IP address for the interface.

	Command or Action	Purpose
Step 5	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 9.3.72.1`	Configure the destination address for UDP broadcasts.
Step 6	**[no] mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the MOP for an interface.
Step 7	**[no] mop sysid** **Example:** `Device(config-apgroup)# [no] mop sysid`	Disables the task of sending MOP periodic system ID messages.



CHAPTER 46

RADIUS Realm

- Information About RADIUS Realm, on page 637
- Enabling RADIUS Realm, on page 638
- Configuring Realm to Match the RADIUS Server for Authentication and Accounting, on page 638
- Configuring the AAA Policy for a WLAN, on page 639
- Verifying the RADIUS-Realm Configuration, on page 641

Information About RADIUS Realm

The RADIUS Realm feature is associated with the domain of the user. Using this feature, a client can choose the RADIUS server through which authentication and accounting is to be processed.

When mobile clients are associated with a WLAN, RADIUS realm is received as a part of Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA) identity response request in the authentication request packet. The Network Access Identifier (NAI) format (EAP-AKA) for WLAN can be specified as *username@domain.com*. The realm in the NAI format is represented after the @ symbol, which is specified as domain.com. If vendor-specific attributes are added as *test*, the NAI format is represented as test@domain.com.

The RADIUS Realm feature can be enabled and disabled on a WLAN. If Realm is enabled on a WLAN, the corresponding user should send the username in the NAI format. The controller sends the authentication request to the AAA server only when the realm, which is in the NAI format and is received from the client, is compiled as per the given standards. Apart from authentication, accounting requests are also required to be sent to the AAA server based on realm filtering.

Realm Support on a WLAN

Each WLAN is configured to support NAI realms. After the realm is enabled on a particular SSID, the lookup is done to match the realms received in the EAP identity response against the configured realms on the RADIUS server. If the client does not send a username with the realm, the default RADIUS server that is configured on the WLAN is used for authentication. If the realm that is received from the client does not match the configured realms on the WLAN, the client is deauthenticated and dropped.

If the RADIUS Realm feature is not enabled on a WLAN, the username that is received as part of the EAP identity request is directly used as the username and the configured RADIUS server is used for authentication and accounting. By default, the RADIUS Realm feature is disabled on WLANs.

- **Realm Match for Authentication**: In dot1x with EAP methods (similar to EAP AKA), the username is received as part of an EAP identity response. A realm is derived from the username and are matched

with the realms that are already configured in the corresponding RADIUS authentication server. If there is a match, the authentication requests are forwarded to the RADIUS server. If there is a mismatch, the client is deauthenticated.

- **Realm Match for Accounting**: A client's username is received through an access-accept message. When accounting messages are triggered, the realm is derived from the corresponding client's username and compared with the accounting realms configured on the RADIUS accounting server. If there is a match, accounting requests are forwarded to the RADIUS server. If there is a mismatch, accounting requests are dropped.

Enabling RADIUS Realm

Follow the procedure given below to enable RADIUS realm:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless aaa policy** *aaa-policy* **Example:** `Device(config)# wireless aaa policy policy-1`	Creates a new AAA policy.
Step 3	**aaa-realm enable** **Example:** `Device(config-aaa-policy)# aaa-realm enable`	Enables AAA RADIUS realm selection. **Note** Use the **no aaa-realm enable** or the **default aaa-realm enable** command to disable the RADIUS realm.

Configuring Realm to Match the RADIUS Server for Authentication and Accounting

Follow the procedure given below to configure the realm to match the RADIUS server for authentication and accounting:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 3	**aaa authorization network default group** *radius-server-group* **Example:** `Device(config)# aaa authorization network default group aaa_group_name`	Sets the authorization method.
Step 4	**aaa authentication dot1x** *realm* **group** *radius-server-group* **Example:** `Device(config)# aaa authentication dot1x cisco.com group cisco1`	Indicates that dot1x must use the realm group RADIUS server.
Step 5	**aaa authentication login** *realm* **group** *radius-server-group* **Example:** `Device(config)# aaa authentication login cisco.com group cisco1`	Defines the authentication method at login.
Step 6	**aaa accounting identity** *realm* **start-stop group** *radius-server-group* **Example:** `Device(config)# aaa accounting identity cisco.com start-stop group cisco1`	Enables accounting to send a start-record accounting notice when a client is authorized, and a stop-record at the end.

Configuring the AAA Policy for a WLAN

Follow the procedure given below to configure the AAA policy for a WLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless aaa policy** *aaa-policy-name* **Example:** `Device(config)# wireless aaa policy aaa-policy-1`	Creates a new AAA policy for wireless.

	Command or Action	Purpose
Step 3	**aaa-realm enable** **Example:** `Device(config-aaa-policy)# aaa-realm enable`	Enables AAA RADIUS server selection by realm.
Step 4	**exit** **Example:** `Device(config-aaa-policy)# exit`	Returns to global configuration mode.
Step 5	**wireless profile policy** *wlan-policy-profile* **Example:** `Device(config)# wireless profile policy wlan-policy-a`	Configures a WLAN policy profile.
Step 6	**aaa-policy** *aaa-policy* **Example:** `Device(config-wireless-policy)# aaa-policy aaa-policy-1`	Maps the AAA policy.
Step 7	**accounting-list** *acct-config-realm* **Example:** `Device(config-wireless-policy)# accounting-list cisco.com`	Sets the accounting list.
Step 8	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 9	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan wlan2 14 wlan-aaa`	Configures a WLAN.
Step 10	**security dot1x authentication-list** *auth-list-realm* **Example:** `Device(config-wlan)# security dot1x authentication-list cisco.com`	Enables the security authentication list for IEEE 802.1x.
Step 11	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 12	**wireless tag policy** *policy* **Example:** `Device(config)# wireless tag policy tag-policy-1`	Configures a policy tag.

	Command or Action	Purpose
Step 13	**wlan** *wlan-name* **policy** *policy-profile* **Example:** `Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a`	Maps a policy profile to the WLAN.
Step 14	**exit** **Example:** `Device(config-policy-tag)# exit`	Returns to global configuration mode.

Verifying the RADIUS-Realm Configuration

Use the following command to verify the RADIUS-realm configuration:

```
Device# show wireless client mac-address 14bd.61f3.6a24 detail


Client MAC Address : 14bd.61f3.6a24
Client IPv4 Address : 9.4.113.103
Client IPv6 Addresses : fe80::286e:9fe0:7fa6:8f4
Client Username : sacthoma@cisco.com
AP MAC Address : 4c77.6d79.5a00
AP Name: AP4c77.6d53.20ec
AP slot : 1
Client State : Associated
Policy Profile : name-policy-profile
Flex Profile : N/A
Wireless LAN Id : 3
Wireless LAN Name: ha_realm_WLAN_WPA2_AES_DOT1X
BSSID : 4c77.6d79.5a0f
Connected For : 26 seconds
Protocol : 802.11ac
Channel : 44
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Re-Authentication Timeout : 1800 sec (Remaining time: 1775 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 06/12/2018 19:52:35 IST
Policy Manager State: Run
```

```
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 25 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : PEAP
VLAN : 113
Multicast VLAN : 0
Access VLAN : 113
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_9040000f
  IIF ID           : 0x9040000F
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 097704090000000DF4607B3B
  Acct Session ID  : 0x00000fa2
  Aaa Server Details
  Server IP        : 9.4.23.50
  Auth Method Status List
       Method : Dot1x
              SM State         : AUTHENTICATED
              SM Bend State    : IDLE
  Local Policies:
       Service Template : wlan_svc_name-policy-profile_local (priority 254)
              Absolute-Timer   : 1800
              VLAN             : 113
  Server Policies:
  Resultant Policies:
              VLAN             : 113
              Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
.
.
.
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```



CHAPTER 47

RADIUS Accounting

- Information About RADIUS Accounting of AP Events, on page 643
- Configuring Accounting Method-List for an AP Profile, on page 643
- Verifying the AP Accounting Information, on page 644
- AAA Accounting, on page 644
- Feature History for Device Ecosystem Data, on page 645
- Information About Device Ecosystem Data, on page 646
- Enable Device Ecosystem Data, on page 646
- Verify Device Ecosystem Data, on page 647

Information About RADIUS Accounting of AP Events

This topic describes the configuration of a RADIUS server to monitor a network with regards to Access Points (APs). Prior to Cisco IOS XE Amsterdam 17.1.1 release, during times of network issues, the controller would not send accounting messages when APs join and disjoin from the controller. From Cisco IOS XE Amsterdam 17.1.1 release onwards, the RADIUS server keeps a record of all the APs that were down and have come up.

Configuring Accounting Method-List for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures the AP profile. The default AP join profile name is *default-ap-profile*.
Step 3	**[no] accounting method-list** *method-list-name* **Example:**	Configures the accounting method list for the AP profile.

	Command or Action	Purpose
	`Device(config-ap-profile)# [no] accounting method-list method-list-name`	Use the **no** form of this command to disable the command.

Verifying the AP Accounting Information

To verify the AP accounting information, use the following command:

```
Device#show wireless stats ap accounting
Base MAC       Total packet Send    Total packet Received Methodlist
-----------------------------------------------------------------------------------------
00b0.e192.0f20     4        3     abc
38ed.18cc.5788     8        8     ML_M
70ea.1ae0.af08     0        0     ML_A
```

To view the details of a method list that is configured for an AP profile, use the following command:

```
Device#show ap profile name Method-list detailed
AP Profile Name               : test-profile
Description                   :
.
.
.
Method-list name              : Method-list
Packet Sequence Jump DELBA    : ENABLED
Lag status                    : DISABLED
.
Client RSSI Statistics
  Reporting                   : ENABLED
  Reporting Interval          : 30 seconds
```

AAA Accounting

Configuring AAA Accounting Using Default Method List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa accounting commands** *privilege_level* **default start-stop group** *group-name* **Example:** `Device(config)# aaa accounting commands 15 default start-stop group group-name`	Creates an accounting method list and enables accounting. • *privilege_level*: AAA accounting level. The valid range is from 0 to 15. • *group-name*: AAA accounting group that supports only TACACS+ group.

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring HTTP Command Accounting Using Named Method List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ip http accounting commands** *level named-accounting-method-list*
	Example:
	`Device(config)# ip http accounting commands 1 oneacct`
		Configures HTTP command accounting using the named method list.
		• *level*: Privilege value from 0 to 15. By default, the following command privilege levels are available on the controller:
		  • *0*: Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands.
		  • *1*: Includes all the user-level commands at the controller prompt (>).
		  • *15*: Includes all the enable-level commands at the controller prompt (>).
		• *named-accounting-method-list*: Name of the predefined command accounting method list.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Feature History for Device Ecosystem Data

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 48: Feature History for Device Ecosystem Data

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Device Ecosystem Data	This feature sends device analytics data in the RADIUS accounting request to Cisco ISE to profile the endpoints.

Information About Device Ecosystem Data

Edge analytics is the process of collecting, processing, and analyzing data from devices in a network. The controller learns about endpoint attributes, such as model number, operating system version, and other information from a set of endpoints using device analytics. The device analytics data is further shared with Cisco Identity Services Engine (ISE) to profile the endpoints. This information sharing is in addition to the DHCP and HTTP attributes already being shared with Cisco ISE using RADIUS accounting messages.

Enable Device Ecosystem Data

Note Before proceeding with the configuration, ensure that device classifier and accounting features are enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a wireless policy profile.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the wireless policy profile.
Step 4	**radius-profiling** **Example:** `Device(config-wireless-policy)# radius-profiling`	Configures client radius profiling.
Step 5	**dot11-tlv-accounting** **Example:**	Configures the controller to send device analytics data that is found in the RADIUS

	Command or Action	Purpose
	`Device(config-wireless-policy)# dot11-tlv-accounting`	accounting request to Cisco ISE in order to profile the endpoints. The **no** form of this command disables the feature.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 7	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Verify Device Ecosystem Data

Use the following command to verify device ecosystem data in RADIUS accounting configuration:

```
Device# show wireless profile policy detailed <name>

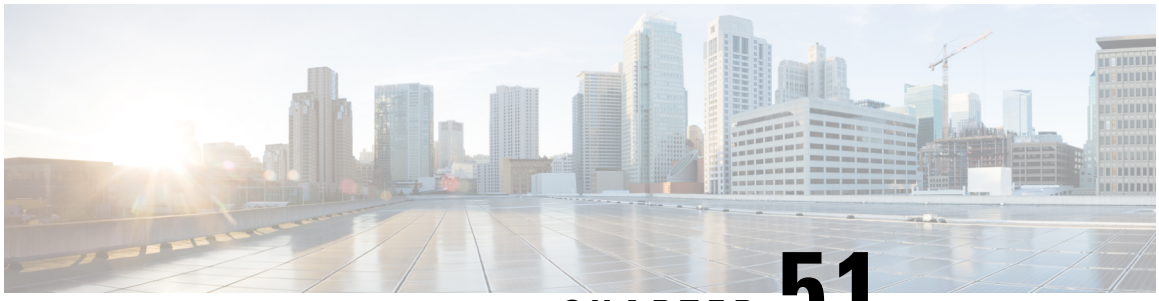
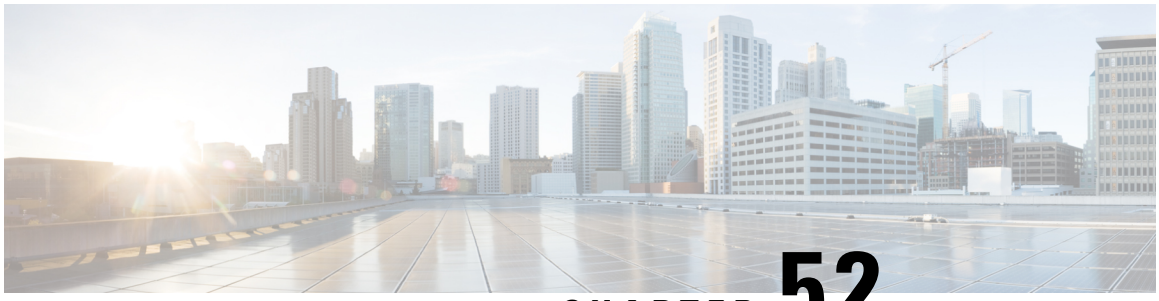
.
.
.
WLAN Local Profiling
  Subscriber Policy Name            : Not Configured
  RADIUS Profiling                  : ENABLED
  HTTP TLV caching                  : DISABLED
  DHCP TLV caching                  : DISABLED
  DOT11 TLV accounting              : ENABLED
.
.
.
```



CHAPTER 48

RADIUS Call Station Identifier

- RADIUS Call Station Identifier, on page 649
- Configuring a RADIUS Call Station Identifier, on page 650

RADIUS Call Station Identifier

The RADIUS called station identifier attribute allows a Network Access Server (NAS) to capture the Access-Request packet used by a phone number by means of Dialled Number Identification (DNIS) or similar technology. The IEEE 802.1X authenticators can use this attribute to store the bridge or Access Point MAC address in ASCII format.

The called station identifier allows a RADIUS server to specify the MAC addresses or networks that a client can connect. One such attribute can be added in the Access-Request packet. The called station identifier is useful in scenarios where preauthentication is supported. In such instances, the called station identifier enables the RADIUS server to restrict the networks and attachment points the client can connect.

Note The called station identifier attribute is applicable only for Access-Request and not for Access-Accept or CoA-Request.

In Cisco IOS XE Bengaluru 17.4.1, the RADIUS called station identifier configuration is enhanced to include more attributes. The newly added options for authentication and accounting are listed below:

- policy-tag-name
- flex-profile-name
- ap-macaddress-ssid-flexprofilename
- ap-macaddress-ssid-policytagname
- ap-macaddress-ssid-sitetagname
- ap-ethmac-ssid-flexprofilename
- ap-ethmac-ssid-policytagname
- ap-ethmac-ssid-sitetagname

For more information on the attributes listed above, see the following commands:

- **radius-server attribute wireless accounting call-station-id**
- **radius-server attribute wireless authentication call-station-id**

Configuring a RADIUS Call Station Identifier

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius-server attribute wireless authentication call-station-id policy-tag-name** **Example:** `Device(config)# radius-server attribute wireless authentication call-station-id policy-tag-name`	Configures a call station identifier sent in the RADIUS authentication messages.
Step 3	**radius-server attribute wireless accounting call-station-id policy-tag-name** **Example:** `Device(config)# radius-server attribute wireless accounting call-station-id policy-tag-name`	Configures a call station identifier sent in the RADIUS accounting messages.



CHAPTER 49

RADIUS VSA

- Information About RADIUS VSA, on page 651
- Create an Attribute List, on page 652
- Create a AAA Policy and Map it to Attribute List, on page 653
- Map a AAA Policy to the WLAN Policy Profile, on page 654
- Map the WLAN Policy Profile to a WLAN, on page 655

Information About RADIUS VSA

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using vendor specific attributes (VSA). VSA allow vendors to support their own extended attributes otherwise not suitable for general use. The controller uses these attributes value in authentication or accounting packets, or both based on specified usage format.

VSA contains these three elements:

- Type
- Length
- String (also known as data)
  - Vendor-ID
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

This feature is supported only in FlexConnect central authentication mode with local switching. FlexConnect local authentication mode is not supported.

This feature is supported only for wireless sessions.

This feature supports the following set of VSAs per WLAN for authentication and accounting requests, in addition to the existing AAA attributes.

Table 49: Newly Supported Attributes

Attribute Name	Well-known Attribute	VSA Sub-attribute	Vendor ID
SVR-Zip-Code	26	14	14369
SVR-Device-Type	26	17	14369
SVR-Device-Model-Number	26	18	14369
SVR-Lat-Long	26	19	14369
SVR-Venue-Category	26	20	14369
SVR-Network-Type	26	21	14369
Aggregation-AAA	26	22	14369
BW-Venue-Id	26	7	22472
BW-Venue-TZ	26	8	22472
BW-Class	26	10	22472
BW-Venue-Description	26	11	22472
BW-ISO-Country-Code	26	14	22472
BW-E164-Country-Code	26	15	22472
BW-State-Name	26	16	22472
BW-City-Name	26	17	22472
BW-Area-Code	26	18	22472
BW-User-Group	26	27	22472
BW-Venue-Name	26	29	22472
BW-Operator-Name	26	37	22472

Create an Attribute List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**aaa attribute list** *list* **Example:** `Device(config)# aaa attribute list TEST`	Creates a AAA attribute list.
Step 3	**attribute type** *attribute-type* **Example:** `Device(config-attr-list)# attribute type BW-City-Name "MUMBAI"`	Specifies a AAA attribute type.
Step 4	**attribute type** *attribute-type* **Example:** `Device(config-attr-list)# attribute type BW-State-Name "MAHARASHTRA`	(Optional) Specifies a AAA attribute type.
Step 5	**attribute type** *attribute-type* **Example:** `Device(config-attr-list)#attribute type BW-Venue-Name "WANKHEDE"`	(Optional) Specifies a AAA attribute type.
Step 6	**end** **Example:** `Device(config-attr-list)# end`	Returns to Privileged EXEC mode.

What to do next

Create a AAA policy and map the attribute list.

Create a AAA Policy and Map it to Attribute List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless aaa policy** *aaa-policy* **Example:** `Device(config)# wireless aaa policy policy-1`	Creates a new AAA policy.
Step 3	**attrlist authentication** *authentication-attr-list* **Example:**	Configures VSA authentication attribute list.

	Command or Action	Purpose
	`Device(config-aaa-policy)# attrlist authentication auth-attr-list`	
Step 4	**attrlist accounting** *accounting-attr-list* **Example:** `Device(config-aaa-policy)# attrlist accounting acct-attr-list`	Configures VSA accounting attribute list.
Step 5	**end** **Example:** `Device(config-aaa-policy)# end`	Returns to Privileged EXEC mode.

What to do next

Map the AAA policy to the WLAN policy profile.

Map a AAA Policy to the WLAN Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy EAP-AKA`	Creates a new wireless policy profile.
Step 3	**aaa-policy** *aaa-policy* **Example:** `Device(config-wireless-policy)# aaa-policy Verizon-aaa-policy`	Creates a new AAA policy.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to Privileged EXEC mode.

What to do next

Map the WLAN policy profile to a WLAN.

Map the WLAN Policy Profile to a WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-name* **Example:** `Device(config)# wireless tag policy EAP-AKA`	Creates a new policy tag.
Step 3	**wlan** *wlan-profile-name* **policy** *aaa-policy* **Example:** `Device(config-policy-tag)# wlan EAP-AKA policy EAP-AKA`	Maps the policy profile to a WLAN.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to Privileged EXEC mode.



CHAPTER 50

Cisco StadiumVision

- Cisco StadiumVision Overview, on page 657
- Configure Parameters for Cisco StadiumVision (GUI), on page 658
- Configure Parameters for Cisco StadiumVision (CLI), on page 658
- Verify StadiumVision Configurations, on page 659

Cisco StadiumVision Overview

Cisco StadiumVision solution is a proven, end-to-end, high-definition IPTV solution that provides advanced digital content management and delivery that can transform the look and feel of venues. It is built on top of the Cisco Connected Stadium solution and centrally-managed through the StadiumVision Director. Cisco StadiumVision solution enables the integration and automated delivery of customized and dynamic content from multiple sources to different areas of the stadium in high definition quality.

This technology allows you to replay certain exciting and critical moments of a game on Wi-Fi capable devices.

To enable Cisco StadiumVision solution on the controller , you need to configure these parameters:

1. On Wireless Controller :
    - Multicast Data Rate
    - RX Sensitivity SOP
    - Multicast Buffer
2. CAPWAP
3. AP Radio Driver and Firmware:
    - Multicast Data Rate
    - RX Sensitivity SOP
    - Multicast Buffer

Configure Parameters for Cisco StadiumVision (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

Step 2 Click the **High Density** tab.

Step 3 In the **Multicast Data Rate** section, set the data rate for 5 GHz radio or 2.4 GHz radio using the drop-down lists.

Step 4 Click **Apply** .

Configure Parameters for Cisco StadiumVision (CLI)

Note Multicast buffer and data rate configurations are supported for all AP models.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *wlan-name wlan-id* **Example:** `Device(config)# wlan wlan1 10`	Configures a WLAN.
Step 2	**multicast buffer** *multicast-buffer-number* **Example:** `Device(config-wlan)# multicast buffer 45`	Configures enhanced multicast buffer size between 30 (default) and 60 on a WLAN. **Note** You can enable only two out of the possible 512 WLANs configured on Controller embedded wireless controller for enhanced multicast buffers.
Step 3	**ap dot11 [5ghz| 24ghz] multicast data-rate** *rate* **Example:** `Device(config)# ap dot11 [5ghz| 24ghz] rx-sop threshold custom -70`	Configures the radio receive sensitivity SOP threshold between -60 to -85 dB, which can also be configured as predefined auto, low, high, medium values specific to 5ghz or 24ghz bands. By default, the configuration is disabled and it's value is set to *auto*. If the RxSOP value of *auto* (0) is pushed, then the AP considers the value burnt-in during manufacturing.

Verify StadiumVision Configurations

- **show ap rf-profile name** *rf-name* **detail**
- **show ap dot11 5ghz** *high-density*

Rx SOP

```
Device#show ap rf-profile name Typical_Client_Density_rf_5gh detail | i SOP
Rx SOP Threshold                 : auto
```

Multicast Buffer

```
Device#show wlan id 1 | sec Buffer
Multicast Buffer                              : Enabled
Multicast Buffer Size                         : 45

Device#

Device#sh wlan name vwlc-OpenAuth | inc Buffer
Multicast Buffer                              : Enabled
Multicast Buffer Size                         : 45
Device#
```

Multicast Data Rate

```
Device#sh ap dot11 24ghz high-density
AP Name                          Mac Address            Slot         Rxsop
Threshold Type Value (dbm)       Multicast Data Rate(Mbps)
-------------------------------------------------------------------------------------
-------------------------------------------------
test-1800-AP                      aaaa.bbbb.cccc            0         auto
        0                         54
AP4001.7AB2.BEB6                  aaab.bbbb.cccc            2         auto
        0                         54
AP70DF.2FA2.72EE                  aaac.bbbb.cccc            0         auto
        0                         0

Device#show ap dot11 5ghz high-density
AP Name                          Mac Address            Slot         Rxsop
Threshold Type Value (dbm)       Multicast Data Rate(Mbps)
-------------------------------------------------------------------------------------
-------------------------------------------------
Saji-1800-AP                      aaab.bbbb.cccc            1         auto
        0                         12
Saji-2802I-AP                     aaab.bbbb.cccc            0         custom
         -82                       12
Saji-2802I-AP                     aaac.bbbb.cccc            1         custom
         -82                       12
AP4001.7AB2.BEB6                  aaad.bbbb.cccc            0         custom
         -82                       12
AP4001.7AB2.BEB6                  aaae.bbbb.cccc            1         custom
         -82                       0
AP500F.8086.8B56                  aaaf.bbbb.cccc            0         custom
         -82                       12
AP500F.8086.8B56                  aaag.bbb.cccc            1         custom
```

```
         -82                          12
AP70DF.2FA2.72EE                  aaah.bbbb.cccc            1         auto
        0                         0

Device#
Device(config)#ap dot11 5ghz rf-profile test_5ghz_rf
Device(config-rf-profile)#high-density multicast data-rate RATE_18M

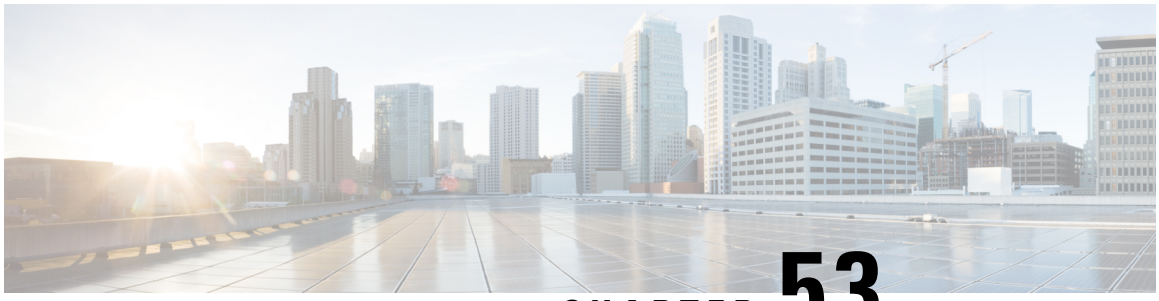
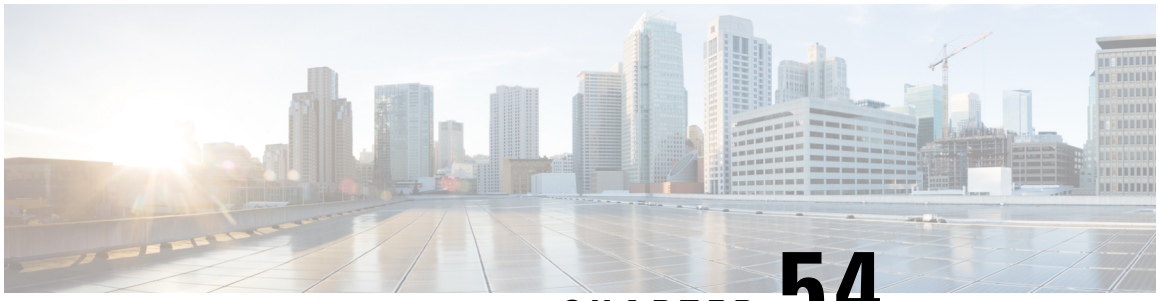
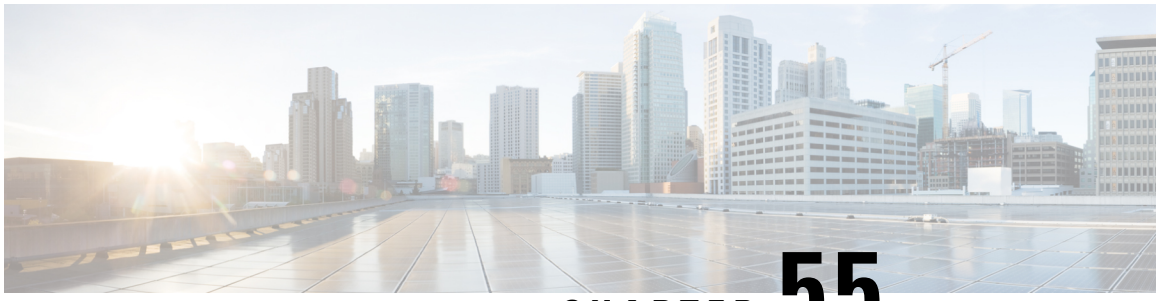
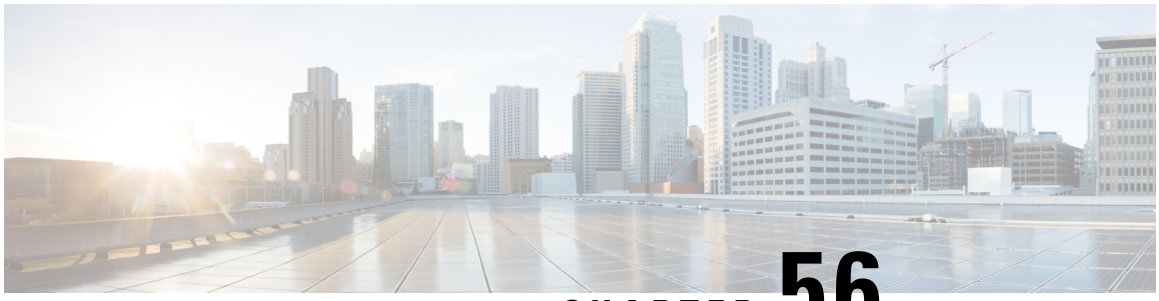
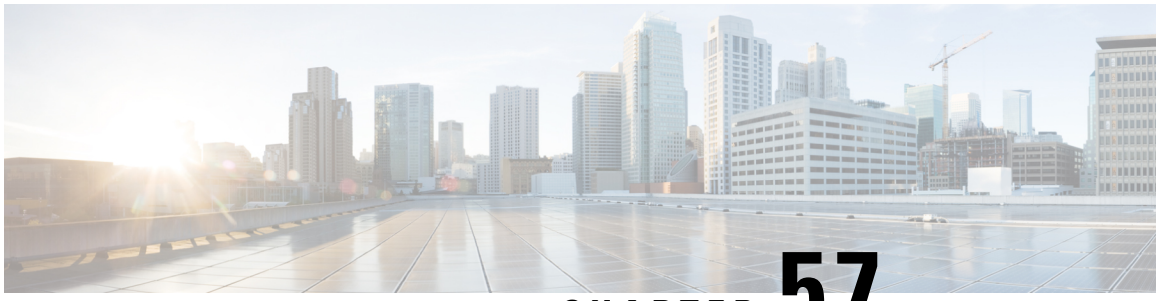
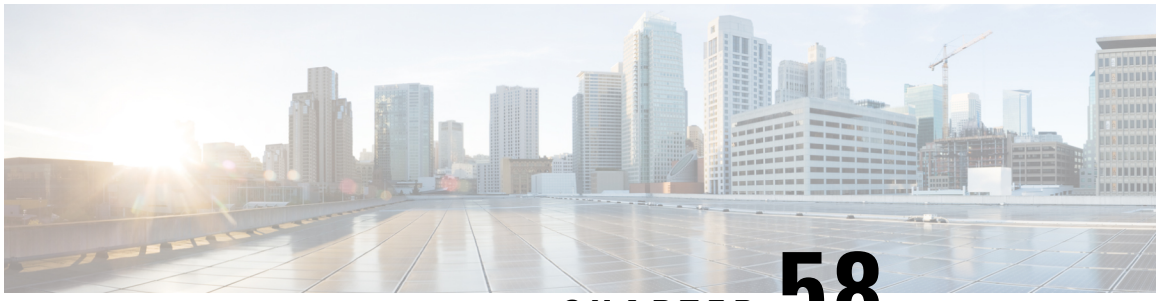
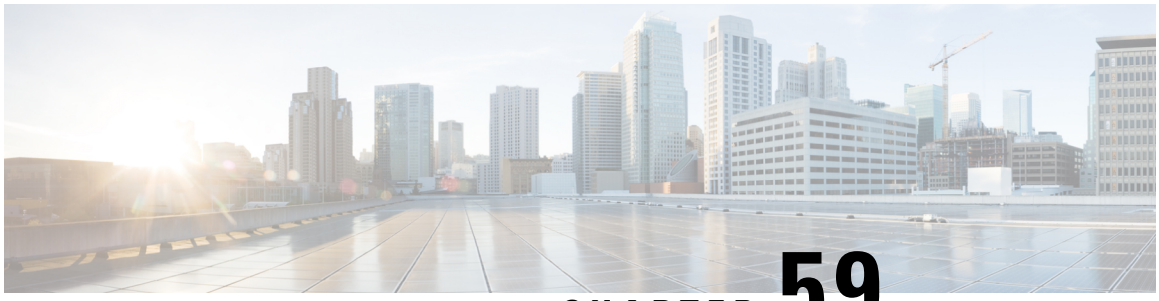

Device#  show ap rf-profile name test_5ghz_rf detail | inc Multicast
Multicast Data Rate               : 18 Mbps
Device#
```



CHAPTER 51

Persistent SSID Broadcast

- Persistent SSID Broadcast, on page 661
- Configuring Persistent SSID Broadcast, on page 661
- Verifying Persistent SSID Broadcast, on page 662

Persistent SSID Broadcast

Access Points within a mesh network work as Root Access Points (RAP) or Mesh Access Points (MAP). RAPs have wired connection to the controller and MAPs have wireless connection to the controller . This feature is applicable only to the Cisco Aironet 1542 Access Points in the Flex+Bridge mode.

This feature is about the Root Access Points (RAPs) and Mesh Access Points (MAPs) broadcasting the SSID even when the WAN connectivity is down. This is required in order to isolate the responsibility; whether the fault is with backhaul or with the access wireless network, since there can be different operators owning each part of the network.

RAPs and MAPs broadcast SSID while in standalone mode, as long as the default gateway is reachable.

Also refer Mesh Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers.

Configuring Persistent SSID Broadcast

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures the AP profile.

	Command or Action	Purpose
Step 3	**[no]ssid broadcast persistent** **Example:** `Device(config-ap-profile)# [no] ssid broadcast persistent`	The **ssid broadcast** command configures the SSID broadcast mode. The **persistent** keyword enables a persistent SSID broadcast, where the associated APs will re-join. Use the **[no]** form of the command to disable the feature. **Note** Enabling or disabling this feature causes the AP to re-join.

Verifying Persistent SSID Broadcast

To view the configuration of all Cisco APs, use the following **show** command:

```
Device#show ap config general
Cisco AP Name   : AP4C77.6DF2.D598
================================================
Office Extend Mode                              : Disabled
Persistent SSID Broadcast                       : Enabled
Remote AP Debug                                 : Disabled
```



CHAPTER 52

Network Monitoring

- Network Monitoring , on page 663
- Status Information Received Synchronously - Configuration Examples, on page 663
- Alarm and Event Information Received Asynchronously - Configuration Examples, on page 665

Network Monitoring

The mechanism that is used to transfer data to the third-party system is NETCONF/YANG. YANG can be used with the Network Configuration Protocol (NETCONF) to provide the desired solution of automated and programmable network operations.

You can contact the API or Developer Support for NETCONF/YANG features using the following link:

https://developer.cisco.com/site/support/#

The two types of information provided are:

- Status information received synchronously - NETCONF is the management interface used for status information, which allows to publish the operational state of the device, including the controller .
- Alarm and event information sent asynchronously - NETCONF/YANG push is the solution used for alarm and event information, which provides the mechanism to send NETCONF notifications subscribed for.

Status Information Received Synchronously - Configuration Examples

NETCONF/YANG interface is used to accomplish customer requests.

The prerequisite configuration for Status Information and Alarm and Event Information is to enable NETCONF server on the controller by using the following command:

netconf-yang

Note The Cisco Catalyst 9800 wireless controller currently only supports RSA keys for the trustpoint used by the ncsshd process. Using EC keys instead of the RSA keys will cause the ncsshd process to crash and it will prevent using NETCONF.

The above command not only enables notifications, but also allows for configuration and operation access (OAM) via Netconf/Yang. For more information on Netconf/Yang, see the *NETCONF Protocol* chapter of the Programmability Configuration Guide at: https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-installation-and-configuration-guides-list.html

In the Status Information Received Synchronously type, the following information is exported though NETCONF:

- Name of the village
- APs in each village
- Status of each AP
- Number of clients currently connected and logged on in each village and each AP

All the data for the items listed above is already available as the controller operational data exported through NETCONF. The examples below explain where the data items listed are available.

The following command is used in the controller :

```
wireless tag site village_name_1
```

The site tags can be retrieved by NETCONF using the **get-config** operation.

Example output for **Name of the Village**:

```
<site-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-site-cfg">
[...]
<site-tag-configs>
  <site-tag-config>
    <site-tag-name>village_name_1</site-tag-name>
    <description>custom user site tag for a village</description>
  </site-tag-config>
[...]
</site-tag-configs>
```

The controller 's operational data contains all the connected (joined) APs and lists their site tags. The example output displays the detailed information about the APs and the site tags. The following example displays the relevant fields and the corresponding controller show commands:

Example output of **Access Point per Village**:

```
<data>
    <access-point-oper-data
xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-oper">
    [...]
      <radio-oper-data>
        <wtp-mac>00:1b:0c:00:02:00</wtp-mac>   #show ap dot11 {24ghz|5ghz} summary "MAC
Address"
        <radio-slot-id>0</radio-slot-id>       #show ap dot11 {24ghz|5ghz} summary "Slot"
        <ap-mac>00:1b:0c:00:02:00</ap-mac>
        <slot-id>0</slot-id>
        <radio-type>1</radio-type>             # 1 - 2.4GHz, 2 - 5GHz
        <admin-state>enabled</admin-state>     #show ap dot11 {24ghz|5ghz} summary "Admin
```

```
State"
        <oper-state>radio-up</oper-state>      #show ap dot11 {24ghz|5ghz} summary "Oper
State"
    [...]
[...]
      <capwap-data>
        <wtp-mac>00:1b:0c:00:02:00</wtp-mac>                #show ap summary  "Radio MAC"
        <ap-operation-state>registered</ap-operation-state> #show ap summary  "State"
        <ip-addr>10.102.140.10</ip-addr>                    #show ap summary  "IP Address"
        [...]
        <admin-state>1</admin-state>              #show ap status   "Status", 1 - Enabled,
 2 - Disabled
        <location>default-location </location>    #show ap summary  "Location"
        <country-code>CH </country-code>
        <name>AP_A-1</name>                       #show ap summary  "AP Name"
 [...]
        <tag-info>
          [...]
          <site-tag>
           <site-tag-name>village_name_1</site-tag-name> #show ap name AP_A-1 config general
 "Site Tag Name"
            [...]
          </site-tag>
[...]
```

The operational data of the controller contains all the connected wireless clients information, which includes detailed client device information, such as the MAC address, IP address, State and the AP name.

Example output of the **Number of clients currently online and logged in each village and each AP**:

```
<data>
    <client-oper-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-client-oper">
      <common-oper-data>
        <client-mac>00:00:1a:04:00:02</client-mac>     #show wireless client summary  "MAC
 Address"
        <ap-name>AP_A-1</ap-name>                      #show wireless client summary  "AP
Name"
        [...]
       <co-state>client-status-run</co-state>        #show wireless client summary  "State"
```

Alarm and Event Information Received Asynchronously - Configuration Examples

The push functionality for the alarm and event information is fulfilled with on-change notifications through NETCONF dynamic subscriptions, with XML encoding.

Example output of **AP Up/Down Events - Subscription**

```
Request:

<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="urn:uuid:b0c581c9-ff5a-4352-9e64-7f2ce1ec603a"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <establish-subscription xmlns="urn:ietf:params:xml:ns:yang:ietf-event-notifications"
   xmlns:yp="urn:ietf:params:xml:ns:yang:ietf-yang-push">
  <stream>yp:yang-push</stream>
```

```
  <yp:xpath-filter>/access-point-oper-data/capwap-data/ap-operation-state</yp:xpath-filter>

  <yp:dampening-period>0</yp:dampening-period>
 </establish-subscription>
</rpc>

Reply:

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:673b42b2-e988-4e20-a6c3-0679c08e6114"><subscription-result
xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'
xmlns:notif-bis="urn:ietf:params:xml:ns:yang:ietf-event-notifications">notif-bis:ok</subscription-result>
<subscription-id
xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'>2147483652</subscription-id>
</rpc-reply>
-->>
(Default Callback)
Event time      : 2018-03-09 15:08:21.880000+00:00
Subscription Id : 2147483651
Type            : 2
Data            :
<datastore-changes-xml xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push">
  <yang-patch xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-patch">
    <patch-id>null</patch-id>
    <edit>
      <edit-id>edit1</edit-id>
      <operation>merge</operation>
      <target>/access-point-oper-data/capwap-data</target>
      <value>
       <capwap-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-oper">

          <ap-operation-state>registered</ap-operation-state>
          <wtp-mac>00ab11006600</wtp-mac>
        </capwap-data>
      </value>
    </edit>
  </yang-patch>
</datastore-changes-xml>
<<--
```



CHAPTER 53

Creating a Lobby Ambassador Account

- Information About Lobby Ambassador Account, on page 667
- Creating a Lobby Ambassador User Account (GUI), on page 667
- Creating a Lobby Ambassador Account (CLI), on page 669

Information About Lobby Ambassador Account

A global administrator can create a lobby ambassador (lobby admin) user for creating guest users.

While creating a guest user, a lobby ambassador can create and delete a guest user, besides setting the following parameters for a guest user:

- Password
- Lifetime of the guest user
- Guest role profiles (Quality-of-Service profiles that should be applied on a guest using the AAA attribute list.

You must ensure that the RADIUS server must be configured with Cisco-AV-pair privilege level with a value greater than zero.

Note You can create a lobby admin from a RADIUS or TACACS server, instead of creating one locally.

Only the admin can create WLAN and web authentication policies. The admin can also create an AAA attribute list, which the lobby admin can use to map to the corresponding guest user.

After an upgrade to Cisco Catalyst 9800 Controller Software release 17.2.x , you must clear the browser cache data to view the lobby admin GUI correctly.

Creating a Lobby Ambassador User Account (GUI)

You can configure administrator or lobby ambassador usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.

Creating a User Account

Procedure

Step 1 From the home page, choose **Administration** > **User Administration**.

Step 2 Click **Add**.

Step 3 In the **User Name** field, enter a user name for the new account.

Step 4 From the **Policy** drop-down list, choose the policy that you want to associate with the user.

Step 5 From the **Privilege** drop-down list, choose the privilege level that you want to associate with the user by clicking the user privilege icon. The following are the options:

- **Go to Basic Mode**
- **Go to Advanced Mode**

Go to Basic Mode: This privilege level defines the commands that users can enter using the CLI after they have logged into the device. Privilege 1 allows access in user EXEC mode and privilege 15 allows access in Privileged EXEC mode.

Go to Advanced Mode:

Admin: Users with Privilege 15 can execute all the **show**, **config**, and **exec** commands on the device. These users will have access to all the sections of the GUI.

Read Only: Users with Privileges 1 to 14 are considered read-only users. The default privilege is 1 if a user is created using the GUI. These users will have access only to the Dashboard and the Monitoring sections.

No Access: Users with Privilege 0 can log in to the device through Telnet or SSH and access the CLI. However, they cannot access the GUI.

Lobby Admin: Users who can create only guest user accounts. While creating a guest user, a lobby ambassador can create and delete a guest user, besides setting the following parameters for a guest user:

- Password
- Lifetime of the guest user
- Guest role profiles (quality-of-service) profiles that should be applied on a guest using the AAA attribute list.

Step 6 In the **Password** field, enter a password for the new account.

Step 7 In the **Confirm Password** field, enter the same password again to reconfirm.

Step 8 Click **Apply to Device**.

Logging In Using the Lobby Account

Note Execute the following commands before logging in using the lobby credentials:

aaa new-model

aaa authorization exec default local

ip http authentication aaa

Logout from the Administrator account and login using the lobby credentials.

You get to view the **Guest User** page.

Creating a Lobby Ambassador Account (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**user-name** *user-name* **Example:** `Device(config)# user-name example-user`	Creates a user account.
Step 3	**type lobby-admin** **Example:** `Device(config-user-name)# type lobby-admin`	Specifies the account type as lobby admin.
Step 4	**password 0** *password* **Example:** `Device(config-user-name)# password 0 example-password`	Creates a password for the lobby administrator account.
Step 5	**aaa attribute list** *user-name* **Example:** `Device(config-user-name)# aaa attribute list example-user`	Creates attribute list for lobby admin access.
Step 6	**attribute type** *wlan-profile-name* **Example:** `Device(config-user-name)# attribute type wlan_wl_mab`	Creates attribute type for lobby admin access.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-user-name)# exit`	Returns to global configuration mode.



CHAPTER 54

Lobby Ambassador Account

- Information About Lobby Ambassador Account, on page 671
- Creating a Lobby Ambassador User Account (GUI), on page 672
- Creating a Lobby Ambassador Account (CLI), on page 673
- Configuring WLAN (GUI), on page 674
- Client Allowed List, on page 675
- Restrictions for Client Allowed List, on page 675
- Creating a Client Allowed List (GUI), on page 675
- Managing Guest Users, on page 676
- Viewing a Client Allowed List, on page 677

Information About Lobby Ambassador Account

A global administrator can create a lobby ambassador (lobby admin) user for creating guest users.

While creating a guest user, a lobby ambassador can create and delete a guest user, besides setting the following parameters for a guest user:

- Password
- Lifetime of the guest user
- Guest role profiles (Quality-of-Service profiles that should be applied on a guest using the AAA attribute list.

You must ensure that the RADIUS server must be configured with Cisco-AV-pair privilege level with a value greater than zero.

Note You can create a lobby admin from a RADIUS or TACACS server, instead of creating one locally.

Only the admin can create WLAN and web authentication policies. The admin can also create an AAA attribute list, which the lobby admin can use to map to the corresponding guest user.

After an upgrade to Cisco Catalyst 9800 Controller Software release 17.2.x , you must clear the browser cache data to view the lobby admin GUI correctly.

Creating a Lobby Ambassador User Account (GUI)

You can configure administrator or lobby ambassador usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.

Creating a User Account

Procedure

Step 1 From the home page, choose **Administration** > **User Administration**.

Step 2 Click **Add**.

Step 3 In the **User Name** field, enter a user name for the new account.

Step 4 From the **Policy** drop-down list, choose the policy that you want to associate with the user.

Step 5 From the **Privilege** drop-down list, choose the privilege level that you want to associate with the user by clicking the user privilege icon. The following are the options:

- **Go to Basic Mode**
- **Go to Advanced Mode**

Go to Basic Mode: This privilege level defines the commands that users can enter using the CLI after they have logged into the device. Privilege 1 allows access in user EXEC mode and privilege 15 allows access in Privileged EXEC mode.

Go to Advanced Mode:

Admin: Users with Privilege 15 can execute all the **show**, **config**, and **exec** commands on the device. These users will have access to all the sections of the GUI.

Read Only: Users with Privileges 1 to 14 are considered read-only users. The default privilege is 1 if a user is created using the GUI. These users will have access only to the Dashboard and the Monitoring sections.

No Access: Users with Privilege 0 can log in to the device through Telnet or SSH and access the CLI. However, they cannot access the GUI.

Lobby Admin: Users who can create only guest user accounts. While creating a guest user, a lobby ambassador can create and delete a guest user, besides setting the following parameters for a guest user:

- Password
- Lifetime of the guest user
- Guest role profiles (quality-of-service) profiles that should be applied on a guest using the AAA attribute list.

Step 6 In the **Password** field, enter a password for the new account.

Step 7 In the **Confirm Password** field, enter the same password again to reconfirm.

Step 8 Click **Apply to Device**.

Logging In Using the Lobby Account

Note Execute the following commands before logging in using the lobby credentials:

aaa new-model

aaa authorization exec default local

ip http authentication aaa

Logout from the Administrator account and login using the lobby credentials.

You get to view the **Guest User** page.

Creating a Lobby Ambassador Account (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**user-name** *user-name* **Example:** `Device(config)# user-name example-user`	Creates a user account.
Step 3	**type lobby-admin** **Example:** `Device(config-user-name)# type lobby-admin`	Specifies the account type as lobby admin.
Step 4	**password 0** *password* **Example:** `Device(config-user-name)# password 0 example-password`	Creates a password for the lobby administrator account.
Step 5	**aaa attribute list** *user-name* **Example:** `Device(config-user-name)# aaa attribute list example-user`	Creates attribute list for lobby admin access.
Step 6	**attribute type** *wlan-profile-name* **Example:** `Device(config-user-name)# attribute type wlan_wl_mab`	Creates attribute type for lobby admin access.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-user-name)# exit`	Returns to global configuration mode.

Configuring WLAN (GUI)

Before you begin

You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 In the **WLANs** window, click the name of the **WLAN** or click **Add** to create a new one.

Step 3 In the **Add/Edit WLAN** window that is displayed, click the **General** tab to configure the following parameters.

- In the **Profile Name** field, enter or edit the name of the profile.
- In the **SSID** field, enter or edit the SSID name.

  The SSID name can be alphanumeric, and up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number. The valid range is between 1 and 512.
- From the **Radio Policy** drop-down list, choose the **802.11** radio band.
- Using the **Broadcast SSID** toggle button, change the status to either **Enabled** or **Disabled** .
- Using the **Status** toggle button, change the status to either **Enabled** or **Disabled** .

Step 4 Click the **Security** tab, and then **Layer 2** tab to configure the following parameters:

- From the **Layer 2 Security Mode** drop-down list, choose **None**. .This setting disables Layer 2 security.
- Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.
- Check the **Over the DS** check box to enable Fast Transition over a distributed system.
- Choose OWE, Opportunistic Wireless Encryption (OWE) provides data confidentiality with encryption over the air between an AP radio and a wireless client. OWE Transition Mode is meant to provide a sort of backwards compatibility.
- Choose Fast Transition, 802.11r which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition.
- Check the check box to enable MAC filtering in the WLAN.
- Check the **Lobby Admin Access** check box to enable Lobby Admin access.

Step 5 Click **Save & Apply to Device**.

Client Allowed List

Clients in universities and hotels need access to networks for a limited period of time. These locations also receive many guests with multiple devices. Therefore it becomes important to protect the networks from misuse or unauthorized access, and allow legitimate clients to connect to the corresponding network.

The client listing feature addresses the need of creating an allowed list for clients on a particular WLAN or SSID- based MAC address.

When you create a new client MAC address as an allowed list user with an invalid WLAN profile name, you must be careful while you map the client MAC to the WLAN profile.

Client allowed list is supported only with MAC addresses that are without a delimiter format.

Two types of administrator roles defined are:

- Global Administrator: Creates a lobby admin user on the controller and enables the lobby administrators access each to the WLAN.
- Lobby Administrator: Adds or deletes a client from the allowed list to manage the association to a WLAN or SSID through the GUI only. Existing lobby administrators can also be used to configure the allowed list.

Restrictions for Client Allowed List

A lobby admin can add clients to allowed list only through the graphical user interface (GUI) and not through the command-line interface (CLI).

Creating a Client Allowed List (GUI)

This section provides multiple methods that you can use as a lobby administrator to create an allowed list for valid users for a WLAN.

Adding Single MAC Address to Allowed List

Procedure

Step 1 Log into Lobby Admin portal.

Step 2 Click **Whitelist Users**.

Step 3 From the drop-down list, choose **WLAN**.

Step 4 Click **Add New Whitelist User**.

Step 5 Select **By MAC Address** radio button.

Step 6 Enter the **MAC address** and **Description**.

Step 7 Click **Apply to Device**.

Adding Bulk MAC Address to Allowed List

Procedure

Step 1 Log into Lobby Admin portal.

Step 2 Click **Whitelist Users**.

Step 3 From the drop-down list, choose the WLAN.

Step 4 Click **Add New Whitelist User**.

Step 5 Select **Bulk Import** radio button.

Step 6 Select the CSV file that lists the clients in MAC Address, Description format.

Step 7 Click **Apply to Device**.

Managing Guest Users

Procedure

Step 1 Log in to Lobby Admin portal using the lobby admin credentials.

Step 2 Click **Whitelist Users**.

Step 3 From the **WLAN**drop-down list, choose the corresponding**WLAN**.

Step 4 From the **WLAN Mode**, select **Onboarding** to enable clients to access the network.

Step 5 Click **Apply.**

Step 6 From the **Connected/Not Whitelisted** in the Whitelist window, select a MAC address . Once the clients join the controller, the MAC addresses are listed in the **Connected/Not Whitelisted**. In the Onboarding mode, MAC filtering in the selected WLAN is disabled. In such a scenario you can change the mode using **Secure** mode.

Step 7 Select **Secure** to automatically add the clients that are connected to the allowed list. In the secure mode, MAC filtering in the selected WLAN is enabled.

Step 8 Click **Apply to Device**.

The clients are listed in the **Connected/Whitelisted**.

Viewing a Client Allowed List

Procedure

Step 1 Log in to the Lobby Admin portal.

Step 2 Click **Whitelist Users**.

Step 3 From the **WLAN**drop-down list, choose the corresponding **WLAN** .

The window lists the following information:

- **Connected/Whitelisted**: Lists the clients that are connected and added to the allowed list by the Lobby admin.
- **Connected/Not Whitelisted**: Lists the clients that are connected, but not added to the allowed list by the Lobby admin.
- **Not Connected/Whitelisted**: Listed the clients that are not connected but added to the allowed list.



CHAPTER 55

Guest User Accounts

- Information About Creating Guest User Accounts, on page 679
- Creating a Guest User Account (GUI), on page 679
- Creating a Guest User Account (CLI), on page 680
- Verifying Guest User Account, on page 681
- Assigning Username to Guest Users in a WLAN (CLI), on page 682

Information About Creating Guest User Accounts

The controller can provide guest user access on WLANs for which you must create guest user accounts. Guest user accounts can be created by network administrators, or, if you would like a non-administrator to be able to create guest user accounts on demand, you can do so through a lobby administrator account. The lobby ambassador has limited configuration privileges and access only to the web pages used to manage the guest user accounts.

The lobby ambassador can specify the amount of time that the guest user accounts remain active. After the specified time elapses, the guest user accounts expire automatically.

You can associate user name with WLAN profile name to restrict guest users in a specific WLAN.

Prerequisites for Guest Users

- Guest users are created by administrator or lobby ambassador.
- Guest user should not have device access either through telnet/ssh or WebUI.
- Guest user should be role-based.
- Guest user should be able to connect to the network and access internet.

Creating a Guest User Account (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Guest User**.

Step 2 On the **Guest User** page, click **Add**.

Step 3 Enter a user name, password, and description for the new account. Check the **Generate password** check box to automatically generate a password.

Step 4 Enter the number of simultaneous user logins. Valid values range between 0 to 64.

Enter 0 for unlimited users.

Step 5 In the **Lifetime** section, choose the number of years, months, days, hours, and minutes.

Step 6 Click **Save & Apply to Device**.

Creating a Guest User Account (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**user-name** *guest-user-name* **Example:** `Device(config)# user-name guest`	Creates a guest user account.
Step 3	**type network-user description** *description* **guest-user max-login-limit** *number of simultaneous logins* **lifetime year** *yy* **month** *mm* **day** *day* **hour** *hour* **minute** *minute* **second** *second* **Example:** `Device(config-user-name)# type network-user description sample-description guest-user max-login-limit 3 lifetime 1 years 0 months 0 days 0 hours 0 mins 0 secs`	Specifies the account type as guest user account.
Step 4	**password 0** *password* **Example:** `Device(config-user-name)# password 0 guest`	Creates a password for the guest user account.
Step 5	**aaa attribute list** *aaa-attribute-list-name* **Example:** `Device(config-user-name)# aaa attribute list aaa-attribute-list-name`	Creates a AAA attribute list to apply QoS profiles on the guest user account.

	Command or Action	Purpose

Step 6	**exit**
	Example:
	`Device(config-user-name)# exit`
		Returns to global configuration mode.
		Note If the lobby admin is local, enter the following command:
		`aaa authentication login default local`
		If the lobby admin is a remote user, enter the following commands:
		`aaa authentication login default group radius/tacacs`
		`aaa remote username <remote-lobby-admin-name>`
		In case of local or remote lobby, enter the following command to map the authorization policies:
		`aaa authorization exec default local`

Verifying Guest User Account

Verify Guest User Account.

```
Device# show aaa local guest_user all
User-Name           : new4
     Type                :  GUEST USER
     Password            : *
     Is_passwd_encrypted : No
     Attribute-List      : Not-Configured
     Viewname            : Not-Configured
     Lobby Admin Name    : NEW_LOBBY_ADMIN
     Max Login Limit     : 0
     Description         : guest
     Start-Time          : 07:56:39 IST Jan 25 2019
     Lifetime            : 1 years 0 months 0 days 0 hours 0 mins 0 secs
     Expiry-Time         : 07:56:39 IST Jan 20 2020 Remaining Lifetime  : 0 years 11 months
 29 days 22 hours 52 mins 49 secs
```

To verify a specific guest user account, use the following command:

```
Device# show aaa local guest_user new_guest3
User-Name           : new_guest3
 Type                :  GUEST USER
 Password            : *
 Is_passwd_encrypted : No
 Attribute-List      : Not-Configured
 Viewname            : Not-Configured
 Lobby Admin Name    : INVALID_ADMIN
 Max Login Limit     : 9
 Description         : new
 Start-Time          : 04:39:01 IST Feb 4 2019
 Lifetime            : 1 years 0 months 0 days 0 hours 0 mins 0 secs
```

```
Expiry-Time         : 04:39:01 IST Jan 30 2020
Remaining Lifetime  : 0 years 11 months 11 days 21 hours 16 mins 34 secs
```

Assigning Username to Guest Users in a WLAN (CLI)

Before you begin

- If wlan-profile-name is configured for a user, guest user authentication is allowed only from that WLAN.
- If wlan-profile-name is not configured for a user, guest user authentication is allowed on any WLAN.
- To work in a connected mode, you need to configure AAA policy override under both SSID policies before assigning a username to a guest user on a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters configuration mode.
Step 2	**username user_name mac wlan-profile-name profile_name** **Example:** `Device(config)# username user_name mac wlan-profile-name profile_name`	Assigns a username to the WLAN profile. **Note** The wlan-profile-name per user is applicable for MAC type users.
Step 3	**show aaa local guest_user new_guest3** **Example:** `Device# show aaa local guest_user new_guest3`	(Optional) Displays the values of the WLAN profile.
Step 4	**end** **Example:** `Device# end`	Returns to privileged EXEC mode.



CHAPTER 56

Link Local Bridging

- Feature History for Link Local Bridging, on page 683
- Information About Link Local Bridging , on page 683
- Use Case for Link Local Bridging, on page 684
- Guidelines and Restrictions for Link Local Bridging, on page 684
- Enabling Link Local Bridging Per Policy Profile (GUI), on page 684
- Enabling Link Local Bridging Per Policy Profile (CLI), on page 685
- Verifying Link Local Bridging, on page 685

Feature History for Link Local Bridging

This table provides release and related information for the feature explained in this module.

This feature is available in all the releases subsequent to the one in which it is introduced in, unless noted otherwise.

Table 50: Feature History for Link Local Bridging

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.6.1	Link Local Bridging	The Link Local Bridging feature allows you to manage link-local traffic in intercontroller and intracontroller roaming scenarios.

Information About Link Local Bridging

In Cisco IOS XE Bengaluru 17.5.1 and earlier releases, client packets were forwarded through the access VLAN of a client. The client also received all the IPv4 or IPv6 packets from its assigned access VLAN.

When an L3 client roamed from one controller to another controller, the point-of-presence (PoP) remained with the first controller, also known as the anchor controller or the home controller, and the point-of-attachment (PoA) moved to the second controller, also known as the foreign controller or the visited controller. In this anchor-foreign scenario, the client packets were tunneled back to the anchor controller to be forwarded on the access VLAN of the client.

Similarly, in case of L3 intracontroller roaming, when the feature Roaming Across Policy Profile is enabled, the client access VLAN is maintained, regardless of the policy profile VLAN. In such a scenario, the PoA becomes the destination policy profile VLAN.

A roaming wireless client is served better by the local services present near its PoA rather than discovering services present at its PoP. Therefore, from Cisco IOS XE Bengaluru 17.6.1 onwards, the intracontroller and intercontroller roaming scenarios described above, can now be managed with the help of the Link Local Bridging feature. Link Local Bridging is disabled by default.

Use Case for Link Local Bridging

If you have a local mode deployment, and L3 roaming is used to manage roaming clients across physical locations, the Link Local Bridging feature helps you to discover services, for example, using mDNS, which are physically close to the wireless client.

Guidelines and Restrictions for Link Local Bridging

- The Link Local Bridging feature is supported in local-mode or FlexConnect central switching.
- Only mDNS bridge mode is supported with Link Local Bridging.
- Guest profiles are not supported.
- Wired Guest LAN, Remote LAN (RLAN), and Inter-Release Controller Mobility (IRCM) are not supported.
- Mesh and IP Source Guard (IPSG) is not supported when the Link Local Bridging feature is enabled.
- Enabling Link Local Bridging on the anchor controller and disabling it on the foreign controller is not supported, even if roaming is successful.
- Access VLAN and bridge VLAN should be operational, for the Link Local Bridging feature to work.
- Link Local Bridging must be enabled across policy profiles for the same SSID.
- Wireless multicast-over-multicast (**wireless multicast** *multicast IP address*) must be configured, before enabling the Link Local Brigding feature. Therefore, the **wireless multicast link-local** command is enabled by default when wireless multicast is enabled.

Enabling Link Local Bridging Per Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.
The **Add Policy Profile** window is displayed.

Step 3 In the **Add Policy Profile** page, in the **General** tab, enter the name of the policy profile.

Step 4 In the **Advanced** tab, check the **Link-Local Bridging** check box to enable link-local bridging on the policy profile.

Note When link-local bridging is enabled, Export Anchor will be disabled and Central Switching will be enabled automatically.

Step 5 Click **Apply to Device**.

Enabling Link Local Bridging Per Policy Profile (CLI)

To enable link local bridging per policy profile, follow these steps.

Before you begin

Ensure that wireless multicast-over-multicast and wireless multicast link-local are enabled.

Note From Cisco IOS XE Bengaluru 17.6.1, the wireless multicast link-local setting is enabled by default as soon as multicast is enabled. This means that all the downstream multicast link-local frames will be forwarded to wireless clients. In the Cisco IOS XE Bengaluru 17.5.x and the earlier releases, only mDNS multicast link-local frames were forwarded.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy wireless-profile1`	Creates policy profile for the WLAN.
Step 3	**link-local-bridging** **Example:** `Device(config-wireless-policy)# link-local-bridging`	Enables link local bridging per policy profile.

Verifying Link Local Bridging

To verify the configuration status of Link Local Bridging, use the following command:

```
Device# show wireless profile policy detailed policy1
Policy Profile Name                : policy1
```

```
Description                          :
Status                               : ENABLED
VLAN                                 : 81
Multicast VLAN                       : 0
OSEN client VLAN                     :
Multicast Filter                     : DISABLED
QBSS Load                            : ENABLED
Passive Client                       : DISABLED
ET-Analytics                         : DISABLED
StaticIP Mobility                    : DISABLED
WLAN Switching Policy
  Flex Central Switching             : ENABLED
  Flex Central Authentication        : ENABLED
  Flex Central DHCP                  : ENABLED
  Flex NAT PAT                       : DISABLED
.
.
.
  ------------------------------------------------------
mDNS Gateway
  mDNS Service Policy name           : default-mdns-service-policy
User Defined (Private) Network              : Disabled
User Defined (Private) Network Unicast Drop  : Disabled
Policy Proxy Settings
  ARP Proxy State                    : DISABLED
  IPv6 Proxy State                   : None
Airtime-fairness Profile
  2.4Ghz ATF Policy                  : default-atf-policy
  5Ghz ATF Policy                    : default-atf-policy
Link-local bridging                  : ENABLED
```

To verify if Link Local Bridging VLAN is included, use the following command:

```
Device# show wireless client mac 7xxx.3xxx.3xxx detail
Client MAC Address : 7xxx.3xxx.3xxx
.
.
.
Link-local bridging VLAN: 3
.
.
.
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
```

To verify if link local multicast traffic is enabled, use the following command:

```
Device# show wireless multicast
Multicast                              : Disabled
AP Capwap Multicast                    : Unicast
Wireless Broadcast                     : Disabled
Wireless Multicast non-ip-mcast        : Disabled
Wireless Multicast link-local          : Enabled
```



CHAPTER 57

Web Admin Settings

- Information About Web Admin Settings, on page 687
- Configuring HTTP/HTTPS Access , on page 687
- Configuring HTTP Trust Point, on page 688
- Configuring Netconf Yang, on page 689
- Configuring Timeout Policy , on page 689
- Configuring VTY, on page 690

Information About Web Admin Settings

This chapter outlines the various settings to access the controller's web interface. These include setting up the controller for communication with others in the network, configuring the management interface to connect over IP, setting up the number of users and protocols to access the controller remotely and configure the source interface for file transfers depending upon the preferred file transfer protocols.

Use the **Administration** > **Management** > **HTTP/HTTPS/Netconf/VTY** page to configure system-wide settings.

Configuring HTTP/HTTPS Access

HTTP/HTTPS access allows users to access the controller's WebUI using its IP address. You can either allow users to connect securely over HTTPS or over HTTP, which is not a secure connection.

Use the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to configure secure access to the controller.

Procedure

Step 1 Enable **HTTP Access** and enter the port that will listen for HTTP requests. The default port is 80. Valid values are 80, and ports between 1025 and 65535.

Step 2 Enable **HTTPS Access** on the device and enter the designated port to listen for HTTPS requests. The default port is 1025. Valid values are 443, and ports between 1025 and 65535.

Enabling HTTPs access allows users to access the controller's GUI using 'https://ip-address' . On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP

with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser.

Step 3 Enable Personal Identity Verification (PIV) for two factor authentication.

This method of authentication allows users to access the WebUI using Personal Identity Verification (PIV) compatible smart cards, enabling login without password. For this to work, ensure that you have configured the trustpoint, CA server certificate on the device and the client certificate signed by the CA server on the browser. Failure to provide the client certificate would deny access to the UI.

Step 4 Set the **Personal Identity Verification Authorization only** option to *Enabled* for authorizing a user's permissions and restrictions based on a remote TACACS+/RADIUS security server.

Step 5 Click **Apply** to save the configuration.

Note In order to use Personal Identity Verification (PIV) for two factor authentication on Safari, perform the following steps.

a. Open Safari browser and go to **Settings > Advanced**

1. Check the **Show Develop in menu bar** check box. This enables the Develop option in the top menu bar.
2. Click **Develop**, and from the dropdown, select **Empty Caches**.

b. Open the web url to login.

Configuring HTTP Trust Point

Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are referred to as trustpoints. When a connection attempt is made, the HTTPS server provides a secure connection by issuing a certified X.509v3 certificate, obtained from a specified CA trustpoint, to the client. The client (usually a Web browser), in turn, has a public key that allows it to authenticate the certificate. For secure HTTP connections, we highly recommend that you configure a CA trustpoint. If a CA trustpoint is not configured for the device running the HTTPS server, the server certifies itself and generates the needed RSA key pair. Because a self-certified (self-signed) certificate does not provide adequate security, the connecting client generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection. This option is useful for internal network topologies (such as testing). If you do not configure a CA trustpoint, when you enable a secure HTTP connection, either a temporary or a persistent self-signed certificate for the secure HTTP server (or client) is automatically generated. If the device is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary new self-signed certificate is assigned. If the device has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the device or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

Use the **Trust Point Configuration**section of the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to make these changes.

Before you begin

You must have configured a trustpoint for web administration purposes.

Procedure

Step 1 Tap to enable the Trust Point.

Step 2 Select the appropriate Trust Point from the drop-down list to to be used for web admin purpose.

If you have not configured a trust point earlier, you can navigate to the appropriate page and first configure it.

Step 3 Click **Apply** to save the configuration.

Configuring Netconf Yang

NETCONF provides a mechanism to install, manipulate, and delete the configuration of network devices.

If the NETCONF connection is configured to use AAA for authentication purposes, it uses only the default Method List and cannot be pointed to use any other named Method List.

Use the **Netconf Yang Configuration** section of the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to make these changes.

Procedure

Step 1 Enable NETCONF.

Step 2 Enter the SSH port number that will be used to facilitate communication between a client and a server. The default port is 830.

Step 3 Click **Apply** to save the configuration.

Configuring Timeout Policy

The Timeout Policy Configuration allows you to configure the details of the interval that the management sessions can remain idle before they timeout. Once the time value is reached, you must log in again to be able to reestablish the connection.

Use the **Timeout Policy Configuration** section of the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to make these changes.

Procedure

Step 1 Enter the maximum number of seconds a connection to the HTTP server should remain open before they timeout in the **HTTP Timeout-policy** field. Once the time value is reached, you must log in again to be able to reestablish connection.

Step 2 Enter the maximum number of seconds the connection will be kept open if no data is received or if response data cannot be sent out on the connection in the **Session Idle Timeout**field

Note that a new value may not take effect on any already existing connections. If the server is too busy or the limit on the life time or the number of requests is reached, the connection may be closed sooner. The default value is 180 seconds (3 minutes).

Step 3 Enter the maximum number of seconds the connection will be kept open, from the time the connection is established in the **Server Life Time** field.

Note that the new value may not take effect on any already existing connections. If the server is too busy or the limit on the idle time or the number of requests is reached, it may close the connection sooner. Also, since the server will not close the connection while actively processing a request, the connection may remain open longer than the specified life time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes. The default value is 180 seconds (3 minutes). The maximum value is 86400 seconds (24 hours).

Step 4 Enter a value for the maximum limit on the number of requests processed on a persistent connection before it is closed in the **Max Number of Requests** field.

Note that the new value may not take effect on already existing connections. If the server is too busy or the limit on the idle time or the life time is reached, the connection may be closed before the maximum number of requests are processed. The default value is 1. The maximum value is 86400.

Step 5 Click **Apply** to save the configuration.

Configuring VTY

VTY is a virtual port used for Telnet or SSH access to the device. VTY is solely used for inbound connections to the device. You can configure the number of simultaneous connections to your device and add security to validate these connections.

Use the **VTY**section of the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to make these changes.

Procedure

Step 1 Set the number of vty lines to allow the number of simultaneous access to the device remotely.

Virtual Terminal Lines or Virtual TeleType (VTY) is a virtual way of accessing the controller 's CLI remotely, unlike physically connecting a laptop to the controller though a console. The number of VTY lines is the maximum number of simultaneous connections possible. 0-50 allows up to fifty simultaneous telnet or ssh sessions to the controller. Although the default is set at 15, we recommend that you to increase the number of VTY lines to 50 to avoid a disruption in connectivity when there are multiple connections to the device.

Step 2 Select the protocol for the remote connection from the **VTY Transport Mode** drop-down list. You can split the connections based on protocol. For e.g. 0-5 might allow for SSH and 10-20 might allow Telnet.

Step 3 (Optional) You can add security in the WebUI to validate login requests. To configure AAA authentication and authorization for inbound sessions to vty lines on your system you must first configure a Radius or a TACACS+ authentication server and select the authentication and authorization list from the corresponding drop-downs.

Step 4 Click **Apply** to save the configuration.



CHAPTER 58

Web UI Configuration Command Accounting in TACACS Server

- Feature History for Web UI Configuration Command Accounting in TACACS+ Server, on page 693
- Information About Web UI Configuration Command Accounting in TACACS+ Server, on page 693
- Guidelines for Web UI Configuration Command Accounting in TACACS+ Server, on page 694
- Configuring AAA Accounting Using Default Method List (CLI), on page 694
- Configuring HTTP Command Accounting Using Named Method List (CLI), on page 695

Feature History for Web UI Configuration Command Accounting in TACACS+ Server

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 51: Feature History for Web UI Configuration Command Accounting in TACACS+ Server

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	Logging Web UI-Based Configuration Changes in TACACS+ Server	This feature logs all configuration changes made in controller web UI. Support for logging configurations done in IOS console in TACACS+ server is already available.

Information About Web UI Configuration Command Accounting in TACACS+ Server

The Cisco Catalyst 9800 Series Wireless Controller configuration is stored in databases. Prior to Cisco IOS XE Cupertino 17.9.1 release, audit log or traceability were not available for the configuration changes stored in databases that were made from the controller GUI. With the Cisco IOS XE Cupertino 17.9.1 release, along with the existing configuration logging of commands executed from Cisco IOS console to TACACS+ server,

support is also added to log the configuration changes done from the controller GUI to TACACS+ server. The logging information includes the command, user, and other session related parameters.

Guidelines for Web UI Configuration Command Accounting in TACACS+ Server

- By default, the configuration commands are not logged to TACACS+ server without configuring command accounting.
- All commands are accounted when AAA default command accounting is configured only for privilege 15.
- When AAA default command accounting is not configured and commands need to be logged in the TACACS+ server, do the following:
  1. The HTTP named method list command accounting.
  2. The AAA named method list (same as the one configured in **Step 1**) command accounting.

Configuring AAA Accounting Using Default Method List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa accounting commands** *privilege_level* **default start-stop group** *group-name* **Example:** `Device(config)# aaa accounting commands 15 default start-stop group group-name`	Creates an accounting method list and enables accounting. • *privilege_level*: AAA accounting level. The valid range is from 0 to 15. • *group-name*: AAA accounting group that supports only TACACS+ group.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring HTTP Command Accounting Using Named Method List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ip http accounting commands** *level named-accounting-method-list*
	Example:
	`Device(config)# ip http accounting commands 1 oneacct`
		Configures HTTP command accounting using the named method list.
		• *level*: Privilege value from 0 to 15. By default, the following command privilege levels are available on the controller:
		  • *0*: Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands.
		  • *1*: Includes all the user-level commands at the controller prompt (>).
		  • *15*: Includes all the enable-level commands at the controller prompt (>).
		• *named-accounting-method-list*: Name of the predefined command accounting method list.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

PART VI

System Management

- Network Mobility Services Protocol, on page 699
- Application Visibility and Control, on page 713
- Software-Defined Application Visibility and Control, on page 735
- Cisco Hyperlocation, on page 739
- FastLocate for Cisco Catalyst Series Access Points, on page 755
- IoT Services Management, on page 759
- IoT Module Management in the Controller, on page 765
- Cisco Spaces, on page 767
- EDCA Parameters, on page 771
- Adaptive Client Load-Based EDCA, on page 775
- 802.11 parameters and Band Selection, on page 779
- NBAR Protocol Discovery, on page 801
- Conditional Debug, Radioactive Tracing, and Packet Tracing, on page 803
- Aggressive Client Load Balancing, on page 815
- Accounting Identity List, on page 819
- Support for Accounting Session ID, on page 823
- Interim Accounting, on page 827
- Wireless Multicast, on page 829
- Map-Server Per-Site Support, on page 849
- Volume Metering, on page 857
- Enabling Syslog Messages in Access Points and Controller for Syslog Server, on page 859
- Login Banner, on page 871
- Wi-Fi Alliance Agile Multiband , on page 873
- SNMP Traps, on page 879

- Disabling Clients with Random MAC Address, on page 885
- Dataplane Packet Logging, on page 889
- Streaming Telemetry, on page 895
- Application Performance Monitoring, on page 915
- Wireless Clients Threshold Warning, on page 921



CHAPTER 59

Network Mobility Services Protocol

- Information About Network Mobility Services Protocol, on page 699
- Radioactive Tracing for NMSP, on page 700
- Enabling NMSP on Premises Services, on page 700
- Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues , on page 701
- Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues, on page 701
- Configuring NMSP Strong Cipher, on page 702
- Verifying NMSP Settings, on page 702
- Examples: NMSP Settings Configuration, on page 705
- NMSP by AP Groups with Subscription List from CMX, on page 705
- Verifying NMSP by AP Groups with Subscription List from CMX, on page 705
- Probe RSSI Location, on page 707
- Configuring Probe RSSI , on page 707
- RFID Tag Support, on page 709
- Configuring RFID Tag Support, on page 709
- Verifying RFID Tag Support, on page 710

Information About Network Mobility Services Protocol

Cisco Network Mobility Services Protocol (NMSP) is a secure two-way protocol that can be run over a connection-oriented (TLS) or HTTPS transport. The wireless infrastructure runs the NMSP server and Cisco Connected Mobile Experiences (Cisco CMX) acts as an NMSP client. The controller supports multiple services and multiple Cisco CMXs can connect to the NMSP server to get the data for the services (location of wireless devices, probe RSSI, hyperlocation, wIPS, and so on.) over the NMSP or HTTPS session.

NMSP defines the intercommunication between Cisco CMX and the controller. Cisco CMX communicates to the controller over a routed IP network. Both publish-subscribe and request-reply communication models are supported. Typically, Cisco CMX establishes a subscription to receive services data from the controller in the form of periodic updates. The controller acts as a data publisher, broadcasting services data to multiple CMXs. Besides subscription, Cisco CMX can also send requests to the controller, causing the controller to send a response back.

The following is a list of the Network Mobility Services Protocol features:

- NMSP is disabled by default.
- NMSP communicates with Cisco CMX using TCP, and uses TLS for encryption.

- Wireless intrusion prevention system (wIPS) is supported only over TCP and TLS.
- Bidirectional communication is supported and Cisco CMX can send a message asynchronously over the established channel.

Note HTTPS is not supported for data transport between controller and Cisco CMX.

Radioactive Tracing for NMSP

This feature collects and provides all CMX-related events.

When a controller is added to CMX with an existing logging or serviceability tools, the following occurs:

- CMX reaches out to the controller through SNMP and CLI.
- Configures the CMX hash key on the controller.
- CMX requests the controller to open an NMSP connection.

RA tracing simplifies troubleshooting by allowing:

- RA trace the CMX IP on the controller.
- Collect all logs about it.

Enabling NMSP on Premises Services

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**nmsp enable** **Example:** `Device(config)# nmsp enable`	Enables NMSP on premises services. **Note** By default, the NMSP is enabled on the controller.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues

NMSP manages communication between the Cisco Connected Mobile Experience (Cisco CMX) and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.

Note The TCP port (16113) that the controller and Cisco CMX communicate over must be open (not blocked) on any firewall that exists between the controller and the Cisco CMX for NMSP to function.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**nmsp notification interval** {**rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } | **spectrum interferers** } *interval*} **Example:** `Device(config)# nmsp notification interval rssi rfid 50`	Sets the NMSP notification interval value for clients, RFID tags, rogue clients, and access points. *interval*-NMSP notification interval value, in seconds for RSSI measurement. Valid range is from 1 to 180.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Modifying the NMSP Notification Threshold for Clients, RFID Tags, and Rogues

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold* **Example:** `Device(config)# location notify-threshold clients 5`	Configures the NMSP notification threshold for clients, RFID tags, rogue clients, and access points. *threshold*- RSSI threshold value in db. Valid range is from 0 to 10, with a default value of 0..
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring NMSP Strong Cipher

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**nmsp strong-cipher** **Example:** `Device(config)# nmsp strong-cipher`	Enable strong ciphers for NMSP server, which contains "ECDHE-RSA-AES128-GCM-SHA256:, ECDHE-ECDSA-AES128-GCM-SHA256:, AES256-SHA256:AES256-SHA:, and AES128-SHA256:AES128-SHA". Normal cipher suite contains, "ECDHE-RSA-AES128-GCM-SHA256:, ECDHE-ECDSA-AES128-GCM-SHA256:, and AES128-SHA".
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying NMSP Settings

To view the NMSP capabilities of the controller , use the following command:

```
Device# show nmsp capability
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
```

```
Spectrum           Aggregate Interferer, Air Quality, Interferer,
Info               Rogue, Mobile Station,
Statistics         Rogue, Tags, Mobile Station,
AP Monitor         Subscription
On Demand Services Device Info
AP Info            Subscription
```

To view the NMSP notification intervals, use the following command:

```
Device# show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 50 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
  Spectrum            : 2 sec
```

To view the connection-specific statistics counters for all CMX connections, use the following command:

```
Device# show nmsp statistics connection
NMSP Connection Counters
------------------------
 CMX IP Address: 10.22.244.31, Status: Active
 State:
      Connections : 1
      Disconnections : 0
      Rx Data Frames : 13
      Tx Data Frames : 99244
      Unsupported messages : 0
  Rx Message Counters:
     ID  Name                                  Count
    ---------------------------------------------
      1  Echo Request                          6076
      7  Capability Notification                  2
     13  Measurement Request                      5
     16  Information Request                      3
     20  Statistics Request                       2
     30  Service Subscribe Request                1

  Tx Message Counters:
     ID  Name                                  Count
    ---------------------------------------------
      2  Echo Response                         6076
      7  Capability Notification                  1
     14  Measurement Response                    13
     15  Measurement Notification             91120
     17  Information Response                     6
     18  Information Notification              7492
     21  Statistics Response                      2
     22  Statistics Notification                305
     31  Service Subscribe Response               1
     67  AP Info Notification                   304
```

To view the common statistic counter of the controller 's NMSP service, use the following command:

```
Device# show nmsp statistics summary
NMSP Global Counters
--------------------
Number of restarts                :

SSL Statistics
--------------------
Total amount of verifications      : 6
```

```
Verification failures              : 6
Verification success               : 0
Amount of connections created      : 8
Amount of connections closed       : 7
Total amount of accept attempts    : 8
Failures in accept                 : 0
Amount of successful accepts       : 8
Amount of failed registrations     : 0

AAA Statistics
--------------------
Total amount of AAA requests       : 7
Failed to send requests            : 0
Requests sent to AAA               : 7
Responses from AAA                 : 7
Responses from AAA to validate     : 7
Responses validate error           : 6
Responses validate success         : 1
```

To view the overall NMSP connections, use the following command:

```
Device# show nmsp status
NMSP Status
-----------

CMX IP Address   Active    Tx Echo Resp  Rx Echo Req   Tx Data     Rx Data     Transport
------------------------------------------------------------------------------------------
127.0.0.1        Active    6             6             1           2           TLS
```

To view all mobility services subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription detail
CMX IP address 127.0.0.1:
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

To view all mobility services subscribed by a specific CMX, use the following command:

```
Device# show nmsp subscription detail <ip_addr>
CMX IP address 127.0.0.1:
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

To view the overall mobility services subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription summary
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

Examples: NMSP Settings Configuration

This example shows how to configure the NMSP notification interval for RFID tags:

```
Device# configure terminal
Device(config)# nmsp notification interval rssi rfid 50
Device(config)# end
Device# show nmsp notification interval
```

This example shows how to configure the NMSP notification interval for clients:

```
Device# configure terminal
Device(config)# nmsp notification interval rssi clients 180
Device(config)# end
Device# show nmsp notification interval
```

NMSP by AP Groups with Subscription List from CMX

The Cisco CMX group support allows you to send only the required Network Mobility Services Protocol (NMSP) data to Cisco CMX (applicable to both on-premises and cloud-based CMX). The Cisco CMX can subscribe to NMSP data of specific APs or AP groups based on the active services in the wireless controller.

This feature helps in load balancing and optimizing the data flow load, when the APs are distributed across different CMX servers. The Cisco CMX server creates a CMX AP group giving it a unique name and groups the APs under it.

Note The Cisco CMX AP Group is the list of Cisco APs managed by the Cisco CMX for location services. This AP group is not the same as the wireless controller AP group.

This feature supports the following services:

- Client
- Probe client filtering
- Hyperlocation
- BLE Services

Note NMSP subscription is available only for those services that are in enabled state in the wireless controller.

Verifying NMSP by AP Groups with Subscription List from CMX

To verify mobility services group subscription summary of all CMX connections, use the following command:

```
Device# show nmsp subscription group summary

CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
```

To view the services that are subscribed for an AP group by a CMX connection, use the following command:

```
Device# show nmsp subscription group details services group-name cmx-IP-addrress

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service            Subservice
-----------------------------
RSSI               Mobile Station,
Spectrum
Info
Statistics
```

To view the AP MAC list that is subscribed for an AP group by a CMX connection, use the following command:

```
Device show nmsp subscription group detail ap-list group-name  cmx-IP-addrress

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 0000.0000.7002  0000.0000.6602  0099.0000.0002  0000.00bb.0002
  0000.0000.5502  0000.0000.5002  0033.0000.0002  00d0.0000.0002
  0010.0010.0002  0000.0006.0002  0000.0002.0002  0000.0000.4002
  0000.0099.0002  0000.0000.a002  0000.7700.0002  0022.0000.0002
  0000.0000.0092  0000.0000.0082  0000.0000.0302  aa00.0000.0002
  0000.0050.0042  0000.0d00.0002  0000.0000.0032  0000.00cc.0002
  0000.0088.0002  2000.0000.0002  1000.0000.0002  0100.0000.0002
  0000.0000.0002  0000.0000.0001  0000.0000.0000
```

To view CMX-AP grouping details for all CMXs, use the following command:

```
Device# show nmsp subscription group detail all
CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
    CMX Group filtered services:
    Service            Subservice
    -----------------------------
    RSSI               Mobile Station,
    Spectrum
    Info
    Statistics

    CMX Group AP MACs:
    : 0000.0000.0003  0000.0000.0002  0000.0000.0001

  Group name: Group2
    CMX Group filtered services:
    Service            Subservice
    -----------------------------
    RSSI               Tags,
    Spectrum
    Info
    Statistics
```

```
    CMX Group AP MACs:
    : 0000.0000.0300  0000.0000.0200  0000.0000.0100

  Group name: Group3
    CMX Group filtered services:
    Service            Subservice
    ----------------------------
    RSSI               Rogue,
    Spectrum
    Info
    Statistics

    CMX Group AP MACs:
    : 0000.0003.0000  0000.0002.0000  0000.0001.0000
```

To view all the AP lists subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription group detail ap-list <group> <cmx-ip>
```

To view all the services subscribed by all CMXs, use the following command:

```
Device# show nmsp subscription group detail services <group> <cmx-ip>
```

Probe RSSI Location

The Probe RSSI Location feature allows the wireless controller and Cisco CMX to support the following:

- Load balancing
- Coverage Hole detection
- Location updates to CMX

When a wireless client is enabled, it sends probe requests to identify the wireless networks in the vicinity and also to find the received signal strength indication (RSSI) associated with the identified Service Set Identifiers (SSIDs).

The wireless client periodically performs active scanning in background even after being connected to an access point. This helps them to have an updated list of access points with best signal strength to connect. When the wireless client can no longer connect to an access point, it uses the access point list stored to connect to another access point that gives it the best signal strength. The access points in the WLAN gather these probe requests, RSSI and MAC address of the wireless clients and forwards them to the wireless controller s. The Cisco CMX gathers this data from the wireless controller and uses it to compute the updated location of the wireless client when it roams across the network.

Configuring Probe RSSI

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless probe filter** **Example:** `Device(config)# wireless probe filter`	Enables filtering of unacknowledged probe requests from AP to improve the location accuracy. Filtering is enabled by default. Use the **no** form of the command to disable the feature. This will forward both acknowledged and unacknowledged probe requests to the controller.
Step 3	**wireless probe limit** *limit-value interval* **Example:** `Device(config)# wireless probe limit 10 100`	Configures the number of probe request reported to the wireless controller from the AP for the same client on a given interval. Use the **no** form of the command to revert to the default limit, which is 2 probes at an interval of 500 ms.
Step 4	**wireless probe locally-administered-mac** **Example:** `Device(config)# wireless probe locally-administered-mac`	Enables the reporting of probes from clients having locally administered MAC address.
Step 5	**location algorithm rssi-average** **Example:** `Device(config)# location algorithm rssi-average`	Sets the probe RSSI measurement updates to a more accurate algorithm but with more CPU overhead.
Step 6	**location algorithm simple** **Example:** `Device(config)# location algorithm simple`	(Optional) Sets the probe RSSI measurement updates to a faster algorithm with smaller CPU overhead, but less accuracy. Use the **no** form of the command to revert the algorithm type to the default one, which is *rssi-average*.
Step 7	**location expiry client** *interval* **Example:** `Device(config)# location expiry client 300`	Configures the timeout for RSSI values. The **no** form of the command sets it to a default value of 15.
Step 8	**location notify-threshold client** *threshold-db* **Example:** `Device(config)# location notify-threshold client 5`	Configures the notification threshold for clients. The **no** form of the command sets it to a default value of 0.
Step 9	**location rssi-half-life client** *time-in-seconds* **Example:** `Device(config)# location rssi-half-life client 20`	Configures half life when averaging two RSSI readings. To disable this option, set the value to 0.

What to do next

Use the **show wireless client probing** command to view each probing client (associated and probing only) by batch of 10 MAC addresses.

RFID Tag Support

The controller enables you to configure radio frequency identification (RFID) tag tracking. RFID tags are small wireless battery-powered tags that continuously broadcast their own signal and are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller , and the Cisco CMX. Only active RFIDs are supported. A combination of active RFID tags and wireless controller allows you to track the current location of equipment. *Active* tags are typically used in real-time tracking of high-value assets in *closed-loop* systems (that is,) systems in which the tags are not intended to physically leave the control premises of the tag owner or originator.

General Guidelines

- You can verify the RFID tags on the controller .
- High Availability for RFID tags are supported.

Configuring RFID Tag Support

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless rfid** **Example:** `Device(config)# wireless rfid`	Enables RFID tag tracking. The default value is enabled. Use the **no** form of this command to disable RFID tag tracking.
Step 3	**wireless rfid timeout** *timeout-value* **Example:** `Device(config)# wireless rfid timeout 90`	Configures the RFID tag data timeout value to cleanup the table. The timeout value is the amount of time that the controller maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.

Verifying RFID Tag Support

To view the summary of RFID tags that are clients, use the following command:

```
Device# show wireless rfid client
```

To view the detailed information for an RFID tag, use the following command:

```
Device# show wireless rfid detail <rfid-mac-address>

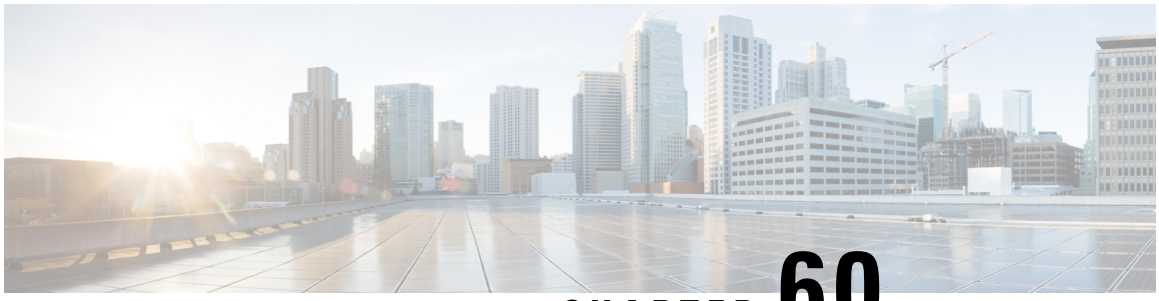
RFID address  000c.cc96.0001
Vendor Cisco
Last Heard 6 seconds  ago
Packets Received 187
Bytes Received 226

Content Header
==============
  CCX Tag Version 0
  Tx power: 12
  Channel: 11
  Reg Class: 4
CCX Payload
==============
  Last Sequence Control 2735
  Payload length 221
  Payload Data Hex Dump:
  00000000  00 02 00 00 01 09 00 00  00 00 0c b8 ff ff ff 02  |................|
  00000010  07 42 03 20 00 00 0b b8  03 4b 00 00 00 00 00 00  |.B. .....K......|
  00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
  00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
  00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

To view the summary information for all known RFID tags, use the following command:

```
Device# show wireless rfid summary

Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 3 minutes 30 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 4 minutes 5 seconds ago
0012.b80b.806c Cisco 7069.5a63.0520 -46 15 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 4 minutes 28 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 4 minutes 29 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 4 minutes 26 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 3 minutes 21 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 4 minutes 28 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 4 minutes 7 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 minute 52 seconds ago
```

To view the location-based system RFID statistics, use the following command:

```
Device# show wireless rfid stats

RFID stats :
==============
RFID error db full : 0
RFID error invalid paylod : 0
RFID error invalid tag : 0
RFID error dot11 hdr : 0
```

```
RFID error pkt len : 0
RFID error state drop : 0
RFID total pkt received : 369
RFID populated error value : 0
RFID error insert records : 0
RFID error update records : 0
RFID total insert record : 16
RFID ccx payload error : 0
RFID total delete record : 0
RFID error exceeded ap count : 0
RFID error record remove : 0
RFID old rssi expired count: 0
RFId smallest rssi expireed count : 0
RFID total query insert : 0
RFID error invalid rssi count : 0
```

To view the NMSP notification interval, use the following command:

```
Device# show nmsp notification interval

NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 50 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
  Spectrum            : 2 sec
```



CHAPTER 60

Application Visibility and Control

- Information About Application Visibility and Control, on page 713
- Create a Flow Monitor, on page 716
- Configuring a Flow Monitor (GUI), on page 718
- Create a Flow Record, on page 718
- Create a Flow Exporter , on page 720
- Configuring a Policy Tag, on page 721
- Attaching a Policy Profile to a WLAN Interface (GUI), on page 722
- Attaching a Policy Profile to a WLAN Interface (CLI), on page 722
- Attaching a Policy Profile to an AP, on page 723
- Verify the AVC Configuration, on page 724
- Default DSCP on AVC, on page 725
- AVC-Based Selective Reanchoring, on page 727
- Restrictions for AVC-Based Selective Reanchoring, on page 728
- Configuring the Flow Exporter, on page 728
- Configuring the Flow Monitor, on page 728
- Configuring the AVC Reanchoring Profile, on page 729
- Configuring the Wireless WLAN Profile Policy , on page 730
- Verifying AVC Reanchoring, on page 731

Information About Application Visibility and Control

Application Visibility and Control (AVC) is a subset of the entire Flexible NetFlow (FNF) package that can provide traffic information. The AVC feature employs a distributed approach that benefits from NBAR running on the access point (AP) or controller whose goal is to run deep packet inspection (DPI) and reports the results using FNF messages.

AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades. Traffic flows are analyzed and recognized using the NBAR2 engine. The specific flow is marked with the recognized protocol or application. This per-flow information can be used for application visibility using FNF. After the application visibility is established, a user can define control rules with policing mechanisms for a client.

Using AVC rules, you can limit the bandwidth of a particular application for all the clients joined on the WLAN. These bandwidth contracts coexist with per-client downstream rate limiting that takes precedence over the per-application rate limits.

FNF feature is supported in wireless, and relies on the NetFlow enablement on the controller for all modes: flex, local and Fabric.

In local mode, the NBAR runs on the controller hardware and the process client traffic flows through the data plane of the controller using the AP CAPWAP tunnels.

In FlexConnect or Fabric mode, NBAR runs on the AP, and only statistics are sent to the controller . When operating in these two modes, APs regularly send FNFv9 reports back to the controller . The controller's FNF feature consumes those FNFv9 reports to provide the application statistics shown by AVC.

The Fabric mode of operation does not populate the FNF cache. It relays the FNFv9 reports at the time they arrive. As a result, some configuration of flow monitors, for example, cache timeout, is not taken into account.

The behavior of the AVC solution changes based on the wireless deployments. The following sections describe the commonalities and differences in all scenarios:

Local Mode

- NBAR is enabled on the controller .
- AVC does not push the FNF configuration to the APs.
- Roaming events are ignored.

  However, AVC supports L3 roams in local mode as traffic flows through the anchor controller (where NBAR was initially processing the roaming client's traffic when the client joined).
- IOSd needs to trigger NBAR attach.
- Supports flow monitor cache.
- Supports NetFlow exporter.

Flex Mode

- NBAR is enabled on an AP
- AVC pushes the FNF configuration to the APs.
- Supports context transfer for roaming in AVC-FNF.
- Supports flow monitor cache.
- Supports NetFlow exporter.

Fabric Mode

- NBAR is enabled on an AP.
- AVC pushes the FNF configuration to the APs.
- Supports context transfer for roaming in AVC-FNF.
- Flow monitor cache is not supported.
- Supports NetFlow exporter (for the C9800 embedded on Catalyst switches for SDA, there is no FNF cache on the box).

Prerequisites for Application Visibility and Control

- The access points should be AVC capable.

  However, this requirement is not applicable in Local mode.

- For the control part of AVC (QoS) to work, the application visibility feature with FNF has to be configured.

Restrictions for Application Visibility and Control

- IPv6 (including ICMPv6 traffic) packet classification is not supported in FlexConnect mode and Fabric mode. However, it is supported in Local mode.
- Layer 2 roaming is not supported across controller controllers.
- Multicast traffic is not supported.
- AVC is supported only on the following access points:
  - Cisco Catalyst 9100 Series Access Points
  - Cisco Aironet 1800 Series Access Points
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 2800 Series Access Point
  - Cisco Aironet 3700 Series Access Points
  - Cisco Aironet 3800 Series Access Points
  - Cisco Aironet 4800 Series Access Points
  - Cisco Industrial Wireless 3702 Access Point
- AVC is not supported on Cisco Aironet 702W, 702I (128 M memory), and 1530 Series access points.
- Only the applications that are recognized with App visibility can be used for applying QoS control.
- Data link is not supported for NetFlow fields in AVC.
- You cannot map the same WLAN profile to both the AVC-not-enabled policy profile and the AVC-enabled policy profile.
- AVC is not supported on the management port (Gig 0/0).
- NBAR-based QoS policy configuration is allowed only on wired physical ports. Policy configuration is not supported on virtual interfaces, for example, VLAN, port channel and other logical interfaces.

When AVC is enabled, the AVC profile supports only up to 23 rules, which includes the default DSCP rule. The AVC policy will not be pushed down to the AP, if rules are more than 23.

AVC Configuration Overview

To configure AVC, follow these steps:

1. Create a flow monitor using the **record wireless avc basic** command.

2. Create a wireless policy profile.
3. Apply the flow monitor to the wireless policy profile.
4. Create a wireless policy tag.
5. Map the WLAN to the policy profile
6. Attach the policy tag to the APs.

Create a Flow Monitor

The NetFlow configuration requires a flow record, a flow monitor, and a flow exporter. This configuration should be the first step in the overall AVC configuration.

Note In Flex mode and Local mode, the default values for **cache timeout active** and **cache timeout inactive** commands are not optimal for AVC. We recommend that you set both the values to 60 in the flow monitor.

For Fabric mode, the cache timeout configuration does not apply.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor fm_avc`	Creates a flow monitor.
Step 3	**record wireless avc** {**ipv4** | **ipv6**} **basic** **Example:**	Specifies the basic IPv4 or IPv6 wireless AVC flow template.

	Command or Action	Purpose
	`Device(config-flow-monitor)# record wireless avc ipv6 basic`	**Note** If you want to have both Application Performance Monitoring (APM) and AVC-FNF in the device simultaneously, use the **record wireless avc {ipv4 | ipv6} assurance** command, which is a superset of the fields contained in **record wireless avc {ipv4 | ipv6} basic** command. If the containing flow monitor is configured with the local exporter using **destination wlc local** command, AVC-FNF will populate the statistics exactly as that of the **record wireless avc {ipv4 | ipv6} basic** configuration. As a result, both APM and AVC-FNF can be configured simultaneously with two flow monitors per direction, per IP version, in local (central switching) mode. **Note** The **record wireless avc basic** command is same as **record wireless avc ipv4 basic** command. However, **record wireless avc ipv4 basic** command is not supported in Flex or Fabric modes. In such scenarios, use the **record wireless avc basic** command.
Step 4	**cache timeout active** *value* **Example:** `Device(config-flow-monitor)# cache timeout active 60`	Sets the active flow timeout in seconds.
Step 5	**cache timeout inactive** *value* **Example:** `Device(config-flow-monitor)# cache timeout inactive 60`	Sets the inactive flow timeout in seconds.

Configuring a Flow Monitor (GUI)

Before you begin

You must have created a flow exporter to export data from the flow monitor.

Procedure

Step 1 Choose **Configuration** > **Services** > **Application Visibility** and go to the **Flow Monitor** tab .

Step 2 In the **Monitor** area, click **Add** to add a flow monitor.

Step 3 In the **Flow Monitor** window, add a flow monitor and a description.

Step 4 Select the Flow exporter from the drop-down list to export the data from the flow monitor to a collector.

Note To export wireless netflow data, use the templates below:

- ETA (Encrypted Traffic Analysis)
- wireless avc basic
- wireless avc basic IPv6

Step 5 Click **Apply to Device** to save the configuration.

Create a Flow Record

The default flow record cannot be edited or deleted. If you require a new flow record, you need to create one and map it to the flow monitor from CLI.

Procedure

	Command or Action	Purpose
Step 1	**flow record** *flow_record_name* **Example:** `Device(config)# flow record record1`	Creates a flow record. **Note** When a custom flow record is configured in Flex and Fabric modes, the optional fields (fields that are not present in record wireless avc basic) are ignored.
Step 2	**description** *string* **Example:** `Device(config-flow-record)# description IPv4flow`	(Optional) Describes the flow record as a maximum 63-character string.

	Command or Action	Purpose
Step 3	**match ipv4 protocol** **Example:** `Device(config-flow-record)# match ipv4 protocol`	Specifies a match to the IPv4 protocol.
Step 4	**match ipv4 source address** **Example:** `Device(config-flow-record)# match ipv4 source address`	Specifies a match to the IPv4 source address-based field.
Step 5	**match ipv4 destination address** **Example:** `Device(config-flow-record)# match ipv4 destination address`	Specifies a match to the IPv4 destination address-based field.
Step 6	**match transport source-port** **Example:** `Device(config-flow-record)# match transport source-port`	Specifies a match to the transport layer's source port field.
Step 7	**match transport destination-port** **Example:** `Device(config-flow-record)# match transport destination-port`	Specifies a match to the transport layer's destination port field.
Step 8	**match flow direction** **Example:** `Device(config-flow-record)# match flow direction`	Specifies a match to the direction the flow was monitored in.
Step 9	**match application name** **Example:** `Device(config-flow-record)# match application name`	Specifies a match to the application name. **Note** This action is mandatory for AVC support because this allows the flow to be matched against the application.
Step 10	**match wireless ssid** **Example:** `Device(config-flow-record)# match wireless ssid`	Specifies a match to the SSID name identifying the wireless network.
Step 11	**collect counter bytes long** **Example:** `Device(config-flow-record)# collect counter bytes long`	Collects the counter field's total bytes.

	Command or Action	Purpose
Step 12	**collect counter packets long** **Example:** `Device(config-flow-record)# collect counter bytes long`	Collects the counter field's total packets.
Step 13	**collect wireless ap mac address** **Example:** `Device(config-flow-record)# collect wireless ap mac address`	Collects the BSSID with the MAC addresses of the access points that the wireless client is associated with.
Step 14	**collect wireless client mac address** **Example:** `Device(config-flow-record)# collect wireless client mac address`	Collects the MAC address of the client on the wireless network.

Create a Flow Exporter

You can create a flow exporter to define the export parameters for a flow. This is an optional procedure for configuring flow exporter parameters.

Note For the AVC statistics to be visible at the controller , you should configure a local flow exporter using the following commands:

- **flow exporter** *my_local*
- **destination local wlc**

Also, your flow monitor must use this local exporter for the statistics to be visible at the controller .

Procedure

	Command or Action	Purpose
Step 1	**flow exporter** *flow-export-name* **Example:** `Device(config)# flow exporter export-test`	Creates a flow monitor.
Step 2	**description** *string* **Example:** `Device(config-flow-exporter)# description IPv4flow`	Describes the flow record as a maximum 63-character string.

	Command or Action	Purpose
Step 3	**destination** {*hostname/ipv4address* | *hostname/ipv6address* |*local {wlc}*} **Example:** `Device(config-flow-exporter)# destination local wlc`	Specifies the hostname or IP address of the system or the local WLC to which the exporter sends data.
Step 4	**transport udp** *port-value* **Example:** `Device(config-flow-exporter)# transport udp 1024`	(Optional) Configures the destination UDP port to reach the external collector. The default value is 9995. **Note** This step is required only for external collectors; not required for local wlc collector.
Step 5	**option application-table timeout** *seconds* **Example:** `Device(config-flow-exporter)# option application-table timeout 500`	(Optional) Specifies the application table timeout option, in seconds. The valid range is from 1 to 86400.
Step 6	**end** **Example:** `Device(config-flow-exporter)# end`	Returns to privileged EXEC mode.
Step 7	**show flow exporter** **Example:** `Device# show flow exporter`	(Optional) Verifies your configuration.

Configuring a Policy Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag`	Configures policy tag and enters policy tag configuration mode.
Step 3	**end** **Example:**	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-policy-tag)# end`	

Attaching a Policy Profile to a WLAN Interface (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page, click **Policy** tab.

Step 3 Click **Add** to view the **Add Policy Tag** window.

Step 4 Enter a name and description for the policy tag.

Step 5 Click **Add** to map WLAN and policy.

Step 6 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.

Step 7 Click **Save & Apply to Device**.

Attaching a Policy Profile to a WLAN Interface (CLI)

Before you begin

- Do not attach different AVC policy profiles on the same WLAN across different policy tags.

  The following is an example of incorrect configuration:

```
wireless profile policy avc_pol1
   ipv4 flow monitor fm-avc1 input
   ipv4 flow monitor fm-avc1 output
   no shutdown
  wireless profile policy avc_pol2
   ipv4 flow monitor fm-avc2 input
   ipv4 flow monitor fm-avc2 output
   no shutdown
  wireless tag policy avc-tag1
   wlan wlan1 policy avc_pol1
  wireless tag policy avc-tag2
   wlan wlan1 policy avc_pol2
```

  This example violates the restriction stated earlier, that is, the WLAN *wlan1* is mapped to 2 policy profiles, *avc_pol1* and *avc_pol2*. This configuration is, therefore, incorrect because the WLAN *wlan1* should be mapped to either *avc_pol1* or *avc_pol2* everywhere.

- Conflicting policy profiles on the same WLAN are not supported. For example, policy profile (with and without AVC) applied to the same WLAN in different policy tags.

  The following is an example of an incorrect configuration:

```
wireless profile policy avc_pol1
   no shutdown
```

```
wireless profile policy avc_pol2
 ipv4 flow monitor fm-avc2 input
 ipv4 flow monitor fm-avc2 output
 no shutdown
wireless tag policy avc-tag1
 wlan wlan1 policy avc_pol1
wireless tag policy avc-tag2
 wlan wlan1 policy avc_pol2
```

In this example, a policy profile with and without AVC is applied to the same WLAN in different tags.

Procedure

	Command or Action	Purpose
Step 1	**wireless tag policy** *avc-tag* **Example:** `Device(config)# wireless tag policy avc-tag`	Creates a policy tag.
Step 2	**wlan** *wlan-avc* **policy** *avc-policy* **Example:** `Device(config-policy-tag)# wlan wlan_avc policy avc_pol`	Attaches a policy profile to a WLAN profile.

What to do next

- Run the **no shutdown** command on the WLAN after completing the configuration.
- If the WLAN is already in **no shutdown** mode, run the **shutdown** command, followed by **no shutdown** command.

Attaching a Policy Profile to an AP

Procedure

	Command or Action	Purpose
Step 1	**ap** *ap-ether-mac* **Example:** `Device(config)# ap 34a8.2ec7.4cf0`	Enters AP configuration mode.
Step 2	**policy-tag** *policy-tag* **Example:** `Device(config)# policy-tag avc-tag`	Specifies the policy tag that is to be attached to the access point.

Verify the AVC Configuration

Procedure

	Command or Action	Purpose
Step 1	**show avc wlan** *wlan-name* **top** *num-of-applications* **applications {aggregate | downstream | upstream}** **Example:** `Device# show avc wlan wlan_avc top 2 applications aggregate`	Displays information about top applications and users using these applications. **Note** Ensure that wireless clients are associated to the WLAN and generating traffic, and then wait for 90 seconds (to ensure the availability of statistics) before running the command.
Step 2	**show avc client** *mac* **top** *num-of-applications* **applications {aggregate | downstream | upstream}** **Example:** `Device# show avc client 9.3.4 top 3 applications aggregate`	Displays information about the top number of applications. **Note** Ensure that wireless clients are associated to the WLAN and generating traffic, and then wait for 90 seconds (to ensure the availability of statistics) before running the command.
Step 3	**show avc wlan** *wlan-name* **application** *app-name* **top** *num-of-clients* **aggregate** **Example:** `Device# show avc wlan wlan_avc application app top 4 aggregate`	Displays information about top applications and users using these applications.
Step 4	**show ap summary** **Example:** `Device# show ap summary`	Displays a summary of all the access points attached to the controller .
Step 5	**show ap tag summary** **Example:** `Device# show ap tag summary`	Displays a summary of all the access points with policy tags.

Default DSCP on AVC

Configuring Default DSCP for AVC Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **QoS**.

Step 2 Click **Add**.

Step 3 Enter the **Policy Name**.

Step 4 Click **Add Class-Maps**.

Step 5 Choose **AVC** in the **AVC/User Defined** drop-down list.

Step 6 Click either **Any** or **All** match type radio button.

Step 7 Choose **DSCP** in the **Mark Type** drop-down list.

Step 8
a) Check the **Drop** check box to drop traffic from specific sources.
b) If you do not want to drop the traffic, enter the **Police(kbps)** and choose the match type from the **Match Type** drop-down list. Choose the items from the available list and click move them to the selected list.

Step 9 Click **Save**.

Step 10 Click **Apply to Device**.

Configuring Default DSCP for AVC Profile

In Cisco Catalyst 9800 Series Wireless Controller, only up to 32 filters can be specified in the policy. As there was no way of classifying the packets that are not specified in the filters, now, you can mark down these packets in the policy.

The marking action can be applied to the traffic when creating a class map and creating a policy map.

Creating Class Map

Procedure

	Command or Action	Purpose
Step 1	**Configure Terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class** *class-map-name*] **Example:** `Device(config-pmap)# class-map avc-class`	Creates a class map.

	Command or Action	Purpose

Step 3	**match protocol** { *application-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application group-name*
	Example:
	`Device(config)# class-map avc-class`
	`Device(config-cmap)# match protocol avc-media`
	`Device(config)# class-map class-avc-category`
	`Device(config-cmap)# match protocol attribute category avc-media`
	`Device# class-map class-avc-sub-category`
	`Device(config-cmap)# match protocol attribute sub-category avc-media`
	`Device# class-map avcS-webex-application-group`
	`Device(config-cmap)# match protocol attribute application-group webex-media`
		Specifies match to the application name, category name, subcategory name, or application group.

Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Creating Policy Map

Procedure

	Command or Action	Purpose
Step 1	**Configure Terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map-name* **Example:** `Device(config)#policy-map avc-policy`	Creates a policy map by entering the policy map name, and enters policy-map configuration mode. By default, no policy maps are defined. The default behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed. **Note** To delete an existing policy map, use the no policy-map policy-map-name global configuration command.

	Command or Action	Purpose
Step 3	**class** [*class-map-name* | **class-default**] **Example:** `Device(config-pmap)# class-map avc-class`	Defines a traffic classification, and enters policy-map class configuration mode. By default, no policy map and class maps are defined. If a traffic class has already been defined by using the class-map global configuration command, specify its name for class-map-name in this command. A class-default traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied match any is included in the class-default class, all packets that have not already matched the other traffic classes will match class-default . **Note** To delete an existing class map, use the no class class-map-name policy-map configuration command.
Step 4	**set dscp** *new-dscp* **Example:** `Device(config-pmap-c)# set dscp 45`	Classifies IP traffic by setting a new value in the packet. For **dscp new-dscp** , enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.
Step 5	**class** *class-default*	Specifies the default class so that you can configure or modify its policy.
Step 6	**set dscp default**	Configures the default DSCP.
Step 7	**end**	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

AVC-Based Selective Reanchoring

The AVC-Based Selective Reanchoring feature is designed to reanchor clients when they roam from one controller to another. Reanchoring of clients prevents the depletion of IP addresses available for new clients in Cisco WLC. The AVC profile-based statistics are used to decide whether a client must be reanchored or deferred. This is useful when a client is actively running a voice or video application defined in the AVC rules.

The reanchoring process also involves deauthentication of anchored clients. The clients get deauthenticated when they do not transmit traffic for the applications listed in the AVC rules while roaming between WLCs.

Restrictions for AVC-Based Selective Reanchoring

- This feature is supported only in local mode. FlexConnect and fabric modes are not supported.
- This feature is not supported in guest tunneling and export anchor scenarios.
- The old IP address is not released after reanchoring, until IP address' lease period ends.

Configuring the Flow Exporter

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**flow exporter** *name* **Example:** `Device(config)# flow exporter avc-reanchor`	Creates a flow exporter and enters flow exporter configuration mode. **Note** You can use this command to modify an existing flow exporter too.
Step 3	**destination local wlc** **Example:** `Device(config-flow-exporter)# destination local wlc`	Sets the exporter as local.

Configuring the Flow Monitor

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor fm_avc`	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. **Note** You can use this command to modify an existing flow monitor too.

	Command or Action	Purpose
Step 3	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter avc-reanchor`	Specifies the name of an exporter.
Step 4	**record wireless avc basic** **Example:** `Device(config-flow-monitor)# record wireless avc basic`	Specifies the flow record to use to define the cache.
Step 5	**cache timeout active** *value* **Example:** `Device(config-flow-monitor)# cache timeout active 60`	Sets the active flow timeout, in seconds.
Step 6	**cache timeout inactive** *value* **Example:** `Device(config-flow-monitor)# cache timeout inactive 60`	Sets the inactive flow timeout, in seconds.

Configuring the AVC Reanchoring Profile

Before you begin

- Ensure that you use the AVC-Reanchor-Class class map. All other class-map names are ignored by Selective Reanchoring.
- During boot up, the system checks for the existence of the AVC-Reanchor-Class class map. If it is not found, default protocols, for example, jabber-video, WiFi-calling, and so on, are created. If AVC-Reanchor-Class class map is found, configuration changes are not made and updates to the protocols that are saved to the startup configuration persist across reboots.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class-map** *cmap-name* **Example:** `Device(config)# class-map AVC-Reanchor-Class`	Configures the class map.

	Command or Action	Purpose
Step 3	**match any** **Example:** `Device(config-cmap)# match any`	Instructs the device to match with any of the protocols that pass through it.
Step 4	**match protocol jabber-audio** **Example:** `Device(config-cmap)# match protocol jabber-audio`	Specifies a match to the application name. You can edit the class-map configuration later, in order to add or remove protocols, for example, jabber-video, wifi-calling, and so on, if required.

Configuring the Wireless WLAN Profile Policy

Follow the procedure given below to configure the WLAN profile policy:

Note Starting with Cisco IOS XE Amsterdam 17.1.1, IPv6 flow monitor is supported on Wave 2 APs. You can attach two flow monitors in a policy profile per direction (input and output) and per IP version (IPv4 and IPv6) in local (central switching) mode, when NBAR runs in the controller. However, only one flow monitor is supported per direction (input and output) and per IP version (IPv4 and IPv6) in FlexConnect and fabric modes on Wave 2 APs, when NBAR runs on the corresponding AP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the policy profile.
Step 4	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Disables central switching.

	Command or Action	Purpose
Step 5	**ipv4 flow monitor** *monitor-name* **input** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor fm_avc input`	Specifies the name of the IPv4 ingress flow monitor.
Step 6	**ipv4 flow monitor** *monitor-name* **output** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor fm_avc output`	Specifies the name of the IPv4 egress flow monitor.
Step 7	**ipv6 flow monitor** *monitor-name* **input** **Example:** `Device(config-wireless-policy)# ipv6 flow monitor fm_v6_avc input`	Specifies the name of the IPv6 ingress flow monitor.
Step 8	**ipv6 flow monitor** *monitor-name* **output** **Example:** `Device(config-wireless-policy)# ipv6 flow monitor fm_v6_avc output`	Specifies the name of the IPv6 egress flow monitor.
Step 9	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

Verifying AVC Reanchoring

Use the following commands to verify the AVC reanchoring configuration:

```
Device# show wireless profile policy detailed avc_reanchor_policy

Policy Profile Name           : avc_reanchor_policy
Description                   :
Status                        : ENABLED
VLAN                          : 1
Wireless management interface VLAN        : 34
!
.
.
.
AVC VISIBILITY                : Enabled
Flow Monitor IPv4
  Flow Monitor Ingress Name   : fm_avc
  Flow Monitor Egress Name    : fm_avc
Flow Monitor IPv6
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
NBAR Protocol Discovery       : Disabled
Reanchoring                   : Enabled
Classmap name for Reanchoring
  Reanchoring Classmap Name   : AVC-Reanchor-Class
```

```
!
.
.
.
  ----------------------------------------------------


Device# show platform software trace counter tag wstatsd chassis active R0 avc-stats debug

Counter Name Thread ID Counter Value
-----------------------------------------------------------------------------
Reanch_deassociated_clients 28340 1
Reanch_tracked_clients 28340 4
Reanch_deleted_clients 28340 3

Device# show platform software trace counter tag wncd chassis active R0 avc-afc debug

Counter Name Thread ID Counter Value
-----------------------------------------------------------------------------
Reanch_co_ignored_clients 30063 1
Reanch_co_anchored_clients 30063 5
Reanch_co_deauthed_clients 30063 4


Device# show platform software wlavc status wncd

Event history of WNCD DB:

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.630342 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822780 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822672 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172073 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738367 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738261 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.162689 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757643 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757542 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.468749 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18857 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18717 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164304 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163877 2 :READY 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593257 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593152 1 :INIT 24:CREATE_FSM 0 0

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
```

```
Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.664772 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822499 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822222 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.207605 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738105 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.737997 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164225 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757266 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757181 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472778 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.15413 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.15263 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164254 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163209 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163189 1 :INIT 24:CREATE_FSM 0 0

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.630764 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822621 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822574 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172357 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738212 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738167 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164048 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757403 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757361 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472561 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18660 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18588 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164293 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163799 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163773 1 :INIT 24:CREATE_FSM 0 0


Device# show platform software wlavc status wncmgrd

Event history of WNCMgr DB:

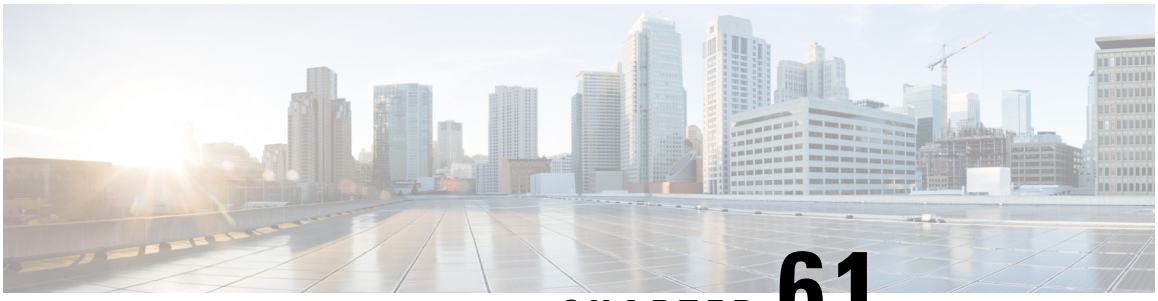
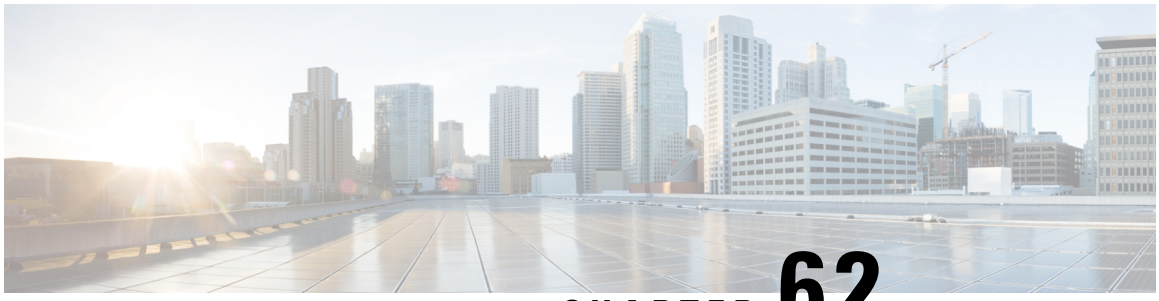
AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.629278 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629223 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629179 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
```

```
06/12/2018 16:45:30.510867 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510411 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510371 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886377 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
!

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------ ------------------------- ---- ----
06/12/2018 16:45:30.664032 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.663958 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.663921 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.511151 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510624 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510608 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.810867 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807239 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807205 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806734 4 :READY 3 :FSM_WLAN_DOWN 0 0
!

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------ ------------------------- ---- ----
06/12/2018 16:45:30.629414 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629392 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629380 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510954 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510572 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510532 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886293 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807844 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807795 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806990 4 :READY 3 :FSM_WLAN_DOWN 0 0
!
```



CHAPTER 61

Software-Defined Application Visibility and Control

- Information About Software-Defined Application Visibility and Control, on page 735
- Enabling Software-Defined Application Visibility and Control on a WLAN (CLI), on page 736
- Configuring Software-Defined Application Visibility and Control Global Parameters (CLI), on page 736

Information About Software-Defined Application Visibility and Control

Software-Defined Application Visibility and Control (SD-AVC) is a network-level AVC controller that aggregates application data from multiple devices and sources and provides composite application information.

SD-AVC collects application data from across the network and deploys protocol pack updates in a centralized manner. SD-AVC recognizes most enterprise network traffic and provides analytics, visibility, and telemetry into the network application recognition. SD-AVC profiles all the endpoints (including wireless bridged virtual machines) connected to the access nodes to perform anomaly detection operations, such as Network Address Translation (NAT). SD-AVC can discover and alert when the same MAC address is used simultaneously on different networks.

You can enable the Software-Defined Application Visibility and Control feature on a per-WLAN basis. Also, you can turn on and turn off the Software-Defined Application Visibility and Control functionalities independently.

Note If the SD-AVC process (stilepd) crashes, Capwapd process restart or AP reload is required to resume the SD-AVC operation.

Enabling Software-Defined Application Visibility and Control on a WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy test-policy-profile`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Disables central switching and enables local switching.
Step 4	**ip nbar protocol-discovery** **Example:** `Device(config-wireless-policy)# ip nbar protocol-discovery`	Enables application recognition on the wireless policy profile by activating the NBAR2 engine.
Step 5	**end** **Example:** `Device(config-wireless-policy)# end`	Exits wireless policy configuration mode and returns to privileged EXEC mode.

Configuring Software-Defined Application Visibility and Control Global Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**avc sd-service** **Example:** `Device(config-sd-service)# avc sd-service`	Enables SD-AVC and enters software-definition service configuration mode.
Step 3	**segment** *segment-name* **Example:** `Device(config-sd-service)# segment AppRecognition`	Configures a segment name identifying a group of devices sharing the same application services.
Step 4	**controller** **Example:** `Device(config-sd-service)# controller`	Enters SD service controller configuration mode to configure connectivity parameters.
Step 5	**address** *ip-address* **Example:** `Device(config-sd-service-controller)# address 209.165.201.0`	Configures controller IP address. Supports only IPv4 address.
Step 6	**destination-ports sensor-exporter** *value* **Example:** `Device(config-sd-service-controller)# destination-ports sensor-exporter 21730`	Configures the destination port for communicating with the controller.
Step 7	**dscp** *dscp-value* **Example:** `Device(config-sd-service-controller)# dscp 16`	Enables DSCP marking.
Step 8	**source-interface** *interface interface-number* **Example:** `Device(config-sd-service-controller)# source-interface GigabitEthernet21`	Configures source interface for communicating with the controller.
Step 9	**transport application-updates https url-prefix** *url-prefix-name* **Example:** `Device(config-sd-service-controller)# transport application-updates https url-prefix cisco`	Configures transport protocols for communicating with the controller.
Step 10	**vrf** *vrf-name* **Example:** `Device(config-sd-service-controller)# vrf doc-test`	Associates the VRF with the source interface.

	Command or Action	Purpose
Step 11	**end** **Example:** `Device(config-sd-service-controller)# end`	Exits the SD service controller configuration mode and enters privileged EXEC mode.



CHAPTER 62

Cisco Hyperlocation

- Information About Cisco Hyperlocation, on page 739
- Restrictions on Cisco Hyperlocation, on page 741
- Support for IPv6 in Cisco Hyperlocation or BLE Configuration, on page 742
- Configuring Cisco Hyperlocation (GUI), on page 742
- Configuring Cisco Hyperlocation (CLI), on page 743
- Configuring Hyperlocation BLE Beacon Parameters for AP (GUI), on page 744
- Configuring Hyperlocation BLE Beacon Parameters for AP (CLI), on page 744
- Configuring Hyperlocation BLE Beacon Parameters (CLI), on page 745
- Information About AP Group NTP Server, on page 746
- Configuring an AP Group NTP Server, on page 746
- Configuring AP Timezone, on page 747
- Information About BLE Concurrent Scanning and Beaconing, on page 747
- Verifying BLE Concurrent Scanning and Beaconing, on page 748
- Verifying Cisco Hyperlocation, on page 749
- Verifying Hyperlocation BLE Beacon Configuration, on page 753
- Verifying Hyperlocation BLE Beacon Configuration for AP, on page 753

Information About Cisco Hyperlocation

Cisco Hyperlocation is an ultraprecise location solution that allows you to track the location of wireless clients. This is possible with the Cisco Hyperlocation radio module in the Cisco Aironet 3600, 3700, and 4800 Series Access Points. The Cisco Hyperlocation module combines Wi-Fi and Bluetooth Low Energy (BLE) technologies to allow beacons, inventory, and personal mobile devices to be pinpointed.

Hyperlocation is also supported in Fabric mode. In particular, when the wireless controller is running on the switch, the controller takes the necessary steps to provision the APs, so that they can generate Hyperlocation VxLAN packets that can traverse the fabric network taking advantage of the fabric infrastructure and be correctly delivered to the destination CMX.

The Hyperlocation VxLAN packets are special packets marked with SGT 0 and using the L3VNID of the APs. For more information, refer to the SDA documentation.

The Cisco Hyperlocation radio module provides the following:

- WSM or WSM2 radio module functions that are extended to:
  - 802.11ac

- Wi-Fi Transmit
- 20-MHz, 40-MHz, and 80-MHz channel bandwidth.

- Expanded location functionality:
  - Low-latency location optimized channel scanning
  - 32-antenna angle of arrival (AoA); available only with the WSM2 module.

Note When using the WSM2 module (includes the WSM module and the antenna add-on), the accuracy of tracking the location of wireless clients can be as close as one meter.

Cisco Hyperlocation works in conjunction with Cisco Connected Mobile Experiences (CMX). Combining the Cisco Hyperlocation feature on Cisco Catalyst 9800 Series Wireless Controller with a CMX device allows you to achieve better location accuracy, which can result in delivering more targeted content to users. When you use CMX with Cisco CleanAir frequency scanning, it is simple to locate failed, lost, and even rogue beacons.

The Cisco Hyperlocation radio module with an integrated BLE radio allows transmission of Bluetooth Low Energy (BLE) broadcast messages by using up to 5 BLE transmitters. Cisco Catalyst 9800 Series Wireless Controller is used to configure transmission parameters such as interval for the beacons, universally unique identifier (UUID), and transmission power, per beacon globally for all the access points. Also, the controller can configure major, minor, and transmission power value of each AP to provide more beacon granularity.

Note The Cisco Hyperlocation feature must be enabled on the controller and CMX and CMX must be connected for BLE to work.

In the absence of a Cisco Hyperlocation radio module, Hyperlocation will still work in a modality named *Hyperlocation Local Mode*, which guarantees a slightly lower location accuracy in the range between five meters and seven meters. This is accomplished through CPU cycle stealing.

Using the controller, you can configure Cisco Hyperlocation for APs based on their profile.

Network Time Protocol Server

Cisco Hyperlocation requires the AP to be synchronized with regard to time. To achieve this, the controller sends network time protocol (NTP) information to the AP. The AP then uses the NTP server to synchronize its clock. Therefore, the AP needs connectivity to the NTP server.

APs can be geographically dispersed. Therefore, it is necessary to provide different NTP servers to different APs. This is achieved by allowing the configuration of NTP server information on a per AP profile basis. If NTP information is not configured on the AP profile, the controller uses one of the global NTP peers defined on its configuration or the management IP address is sent as the NTP server to be used if the controller is acting as an NTP server. If the NTP server is not available, Cisco Hyperlocation will be disabled.

Note In scale setup, the NTP server should be configured on the respective AP profiles, so that the APs and CA servers used for LSC provisioning are time synchronized. If the NTP server is not configured, a few APs would fail in LSC provisioning.

Bluetooth Low Energy Configuration

The BLE configuration is split into two parts: per-AP profile and per AP. The BLE feature can be configured partially from the AP profile (by default, the AP profile BLE configuration is applied) and partially per-AP (some or all the attributes are applied).

Table 52: BLE Configuration Details

Attribute	BLE Configuration Per AP Profile	BLE Configuration Per AP
Attributes with per-AP granularity (global for all the beacons)	• Interval • Advertised transmission power	• Interval • Advertised transmission power
Attributes with per-AP per0-beacon granularity	• Transmission power • UUID • Status	• Transmission power • UUID • Status • Major • Minor

Note The *default-ap-profile* BLE configuration can be considered the default BLE configuration because all the APs will join the *default-ap-profile* AP profile in case the other profiles are removed.

For more information about Cisco Hyperlocation, see the following documents:

- Cisco Hyperlocation Solution
- Cisco CMX Configuration Guide to enable Cisco Hyperlocation
- Cisco CMX Release Notes

Restrictions on Cisco Hyperlocation

- It is not possible to modify detection, trigger, and reset thresholds while Hyperlocation is in enabled state.
- Changes to the reset threshold are allowed for values in the range of zero to one less than the current threshold value. For example, if the current threshold reset value is 10, changes to the reset threshold are allowed for values in the range of 0 to 9.

- When Cisco Hyperlocation is in use on the Cisco Catalyst 9800 Series Wireless Controller in a non-Fabric deployment, CMX must be reachable through an SVI interface (VLAN). Deployments where CMX is reachable through an L3 port results in an error.
- In Fabric deployments, the wireless management interface (typically loopback interface) must not be in Fabric.
- It is not possible to set the wireless management interface to a loopback interface in non-Fabric deployments.

Support for IPv6 in Cisco Hyperlocation or BLE Configuration

Until Release 16.12, IPv4 was the only valid configuration. From Release 17.1 onwards, IPv6 is also supported for specific deployments.

Note CMX accepts only one IP configuration at a time (either IPv4 or IPv6).

The configuration combinations listed in the following tables are the valid deployments.

Table 53: Flex Deployment Mode

Controller Management Inferface and AP	CMX
IPv4	IPv4
IPv6	IPv6

Table 54: Fabric Deployment Mode

Controller Management Inferface and AP	CMX
IPv4	IPv4

Note Any other combination of IPv4 or IPv6 is not supported.

Configuring Cisco Hyperlocation (GUI)

Cisco Hyperlocation is a location solution that allows to track the location of wireless clients with the accuracy of one meter. Selecting this option disables all other fields in the screen, except NTP Server.

Procedure

Step 1 In the **Configuration > Tags & Profiles > AP Join** page, click **Add**.

The **Add AP Join Profile** dialog box appears.

Step 2 Under the **AP** > **Hyperlocation** tab, select the **Enable Hyperlocation** check box.

Step 3 In the **Detection Threshold (dBm)** field, enter a value to filter out packets with low RSSI. You must enter a value between –100 dBm and –50 dBm.

Step 4 In the **Trigger Threshold (cycles)** field, enter a value to set the number of scan cycles before sending a BAR to clients. You must enter a value between 0 and 99.

Step 5 In the **Reset Threshold is required** field, enter a value to reset value in scan cycles after trigger. You must enter a value between 0 and 99.

Step 6 Click **Save & Apply to Device**.

Configuring Cisco Hyperlocation (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile profile-name`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**[no] hyperlocation** **Example:** `Device(config-ap-profile)# [no] hyperlocation`	Enables Cisco Hyperlocation feature on all the supported APs that are associated with this AP profile. Use the **no** form of the command to disable the Cisco Hyperlocation feature.
Step 4	**[no] hyperlocation threshold detection** *value-in-dBm* **Example:** `Device(config-ap-profile)# [no] hyperlocation threshold detection -100`	Sets threshold to filter out packets with low RSSI. The **no** form of this command resets the threshold to its default value. Valid range is between –100 and –50.
Step 5	**[no] hyperlocation threshold reset** *value-btwn-0-99* **Example:** `Device(config-ap-profile)# [no] hyperlocation threshold reset 8`	Resets the value of scan cycles after a trigger. The **no** form of this command resets the threshold to its default value.
Step 6	**[no] hyperlocation threshold trigger** *value-btwn-1-100*	Sets the number of scan cycles before sending a block acknowledgment request (BAR) to

	Command or Action	Purpose
	Example: `Device(config-ap-profile)# [no] hyperlocation threshold trigger 10`	clients. The **no** form of this command resets the threshold to its default value.
Step 7	**[no] ntp ip** *ip-address* **Example:** `Device(config-ap-profile)# [no] ntp ip 9.0.0.4`	Sets the IP address of the NTP server. The **no** form of this command removes the NTP server.

Configuring Hyperlocation BLE Beacon Parameters for AP (GUI)

Procedure

Step 1 In the **Configuration > Tags & Profiles > AP Join** page, click **Add**.

The **Add AP Join Profile** dialog box appears.

Step 2 Under the **AP** tab, click **BLE**.

Step 3 In the **Beacon Interval (Hz)** field, enter a value.

Step 4 In the **Advertised Attenuation Level (dBm)** field, enter a value.

Step 5 Select the check box against each ID and click **Reset**, if required.

Step 6 Optional, click an ID to edit the values of the following fields, and click **Save**.

- **Status**
- **Tx Power (dBm)**
- **UUID**

Step 7 Click **Save & Apply to Device**.

Configuring Hyperlocation BLE Beacon Parameters for AP (CLI)

Follow the procedure given below to configure hyperlocation BLE beacon parameters for an AP:

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **hyperlocation ble-beacon** *beacon-id* { **enable** | **major** *major-value* | **minor** *minor-value* | **txpwr** *value-in-dBm* | **uuid** *uuid-value* }	Configures Hyperlocation and related parameters for an AP, and the specified beacon ID: • **enable**—Enables BLE beacon on the AP.

	Command or Action	Purpose
	Example: `Device# ap name test-ap hyperlocation ble-beacon 3 major 65535`	• **major** *major-value*—Configures BLE beacon's major parameter. Valid value is between 0 and 65535; the default value is 0. • **minor** *minor-value*—Configures BLE beacon's minor parameter. Valid value is between 0 and 65535; the default value is 0. • **txpwr** *value-in-dBm*—Configures BLE beacon attenuation level. Valid value is between –52 dBm and 0 dBm. • **uuid** *uuid-value*—Configures a UUID.
Step 2	**ap name** *ap-name* **hyperlocation ble-beacon advpwr** *value-in-dBm* **Example:** `Device# ap name test-ap hyperlocation ble-beacon advpwr 90`	Configures BLE beacon's advertised attenuation level for an AP. The valid range for *value-in-dBm* is between –40 dBm and –100 dBm; the default value is –59 dBm (all values must be entered as positive integers).

Configuring Hyperlocation BLE Beacon Parameters (CLI)

Before you begin

For Hyperlocation BLE to be enabled, CMX must be fully joined and enabled for Hyperlocation.

Procedure

	Command or Action	Purpose
Step 1	**ap profile** *profile-name* **Example:** `Device(config)# ap profile profile-name`	Enables configuration for all the APs that are associated with the specified AP profile name.
Step 2	**hyperlocation ble-beacon** *beacon-id* **Example:** `Device(config-ap-profile)# hyperlocation ble-beacon 3`	Specifies the BLE beacon parameters and enters BLE configuration mode.
Step 3	**enabled** **Example:** `Device(config-halo-ble)# enabled`	Enables BLE for the beacon ID specified.
Step 4	**exit** **Example:**	Returns to AP profile configuration mode.

	Command or Action	Purpose
	`Device(config-halo-ble)# exit`	
Step 5	**hyperlocation ble-beacon interval** *value-in-hertz* **Example:** `Device(config-ap-profile)# hyperlocation ble-beacon interval 1`	Configures the BLE beacon interval as 1 Hz for the selected profile.
Step 6	**hyperlocation ble-beacon advpwr** *value-in-dBm* **Example:** `Device(config-ap-profile)# hyperlocation ble-beacon advpwr 40`	Configures the BLE beacon-advertised attenuation level. Valid range is between –40 dBm and –100 dBm. The default value is –59 dBm.

Information About AP Group NTP Server

Features such as Cisco Hyperlocation, BLE Angle of Arrival (AoA), and Intelligent Capture (iCAP) require precise time across APs within an AP group to achieve location accuracy. Because the controller and controller global NTP server are configured on the WAN, they might have large synchronization delays from the APs, and this might compromise location accuracy.

If all the APs in an AP group synchronize with the same NTP server, accurate data can be obtained to calculate the location. Configuring the NTP server locally for all the APs in an AP group helps achieve better synchronization among APs.

Configuring an AP Group NTP Server

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile profile-name`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**[no] ntp ip** *ip-address* **Example:** `Device(config-ap-profile)# [no] ntp ip 9.0.0.4`	Sets the IP address of the NTP server. The **no** form of this command removes the NTP server.

	Command or Action	Purpose
Step 4	**[no] ntp auth-key** *key-index* **type** *type* **format** *format* **key** *encryption-type server-key* **Example:** `Device(config-ap-profile)# ntp auth-key index 1 type md5 format ascii key 0 3434324`	Configures NTP server per AP profile to support authentication. The **no ntp auth-key** command removes the NTP server from each AP profile. **Note** For ASCII key, ensure that the length is less than 21 bytes. For HEX key, the length should be less than 41, using only numbers between 0-9 and characters from a-f.

Configuring AP Timezone

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile test`	Configures the AP profile and enters AP profile configuration mode.
Step 3	**timezone** {**use-controller** | **delta hour** *offset-hour* **minute** *offset-minute*} **Example:** `Device(config-ap-profile)# timezone delta hour -12 minute 2`	Configures the timezone offset for AP. You can configure the AP timezone only for each AP profile. You cannot configure timezone for each AP. To configure the timezone, either apply the current controller timezone or the time difference. By default, timezone is disabled.

Information About BLE Concurrent Scanning and Beaconing

From Cisco IOS XE Cupertino 17.9.1, Cisco Catalyst Wi-fi6 APs in basic mode or Cisco IOx mode support concurrent scanning and beaconing. The BLE radio on an AP can stop a scan for beacon transmission and return to the scan after completing the beacon transmission.

This feature is supported only on Cisco Catalyst 9105ax, 9120ax, 9124, 9130, 9136, and Cisco Catalyst 916x APs.

BLE concurrent scanning and beaconing can be enabled from Cisco Spaces using the **Dual** mode under **Device Management** > **AP Beacon** > **Settings**.

Note BLE concurrent scanning and beaconing is not supported when v-IBeacon is used. Supported advertisement profiles are iBeacon, Eddystone-URL, and Eddystone-UID.

Verifying BLE Concurrent Scanning and Beaconing

Use the following commands to verify the status of concurrent scanning and beaconing.

To display the advertisement profile, scan counters, and advertisement counters along with other information, use the following command from the AP console:

```
Device# show controllers IOTRadio ble 0 interface

Active BLE host interface       : /dev/ttyiot0
BLE Radio Status                : Powered on
Device Status                   : Open
Device Mode                     : Native
Device resets                   : 4
Last Reset Reason               : Watchdog Timer Reset
Heart beat status               : On
Scan Status                     : Enabled
Active Transmit Profile         : Eddystone URL
BLE MAC                         : 80:6F:B0:31:EF:74
Transmitted advertisement count
 since BLE enabled              : 0
Total scan records received     : 3617
```

To see whether the transmit profile configuration has been successfully pushed from Cisco Spaces to the AP, use the following command from the AP console:

```
Device# show controllers iOTRadio ble 0 broadcast

BLE Profile Config
------------------
Active profile           : Eddystone UID
Profile 0 (iBeacon)
UUID                     : 00000001023012120312032130012111
Interval (ms)            : 100
Power (dBm)              : 0
Advertised Power (dBm)   : -45
Minor                    : 29219
Major                    : 35826
TxPower byte             :

Profile 1 (Eddystone UID)
Namespace (hex)          : 00000000000000000999
Instance-ID (hex)        : 000000000555

Profile 2 (Eddystone URL)
URL                      :

Profile 3 (v-iBeacon)
v-iBeacon status         : Disabled
Chirping interval (ms)   : 100
Profile 4 (Custom Profile)
Adv Data                 :
0000000000000000000000000000000000000000000000000000000000000000
Scan Data                :
```

```
00000000000000000000000000000000000000000000000000000000000000000000
Simulator mode           : Disabled
Beacon-ID               Mac                                 UUID Major Minor Status
        1 10:F9:20:FE:1D:8F 00000000000000000000000000000000     0     0      0
        2 10:F9:20:FE:1D:8E 00000000000000000000000000000000     0     0      0
        3 10:F9:20:FE:1D:8D 00000000000000000000000000000000     0     0      0
        4 10:F9:20:FE:1D:8C 00000000000000000000000000000000     0     0      0
        5 10:F9:20:FE:1D:8B 00000000000000000000000000000000     0     0      0

Beacon-ID Transmit power(dBm) Advertised power(dBm)
        1                -21                -256
        2                -21                -256
        3                -21                -256
        4                -21                -256
        5                -21                -256
```

To view the list of joined APs that support the BLE Management feature along with the BLE details for each AP, use the following command from the controller:

```
Device# show ap ble summary

AP Name AP Model   AP Ethernet MAC BLE      BLE    BLE mode      BLE MAC        BLE Profile
     BLE Scan
                                   Interface Admin
                                   State     State
-------------------------------------------------------------------------------------------------------
AP794   C9130AXI-B 04eb.409e.xxxx  Open      Up     Base (Native) 806f.b031.xxxx  Eddystone
 URL   Enabled
AP50    C9130AXI-B 04eb.409e.xxxx  Close     Down   Base (Native) Unknown         Not
Configured  Disabled
AP28    C9136I     687d.b45c.xxxx  Close     Down   Base (Native) Unknown         Not
Configured  Disabled
```

Verifying Cisco Hyperlocation

To display the hyperlocation status values and parameters for all the AP profiles, use the following command:

```
Device# show ap hyperlocation summary

Profile Name: custom-profile

Hyperlocation operational status: Down
Reason: Hyperlocation is administratively disabled
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Disabled
Hyperlocation detection threshold (dBm): -100
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8


Profile Name: default-ap-profile

Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 22
Hyperlocation reset threshold: 8
```

To display both the overall and the per-AP configuration values and operational status, use the following command:

```
Device# show ap hyperlocation detail

Profile Name: house24

Hyperlocation operational status: Up
 Reason: NTP server is not properly configured
Hyperlocation NTP server: 198.51.100.1
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7

AP Name                 Radio MAC         Method      CMX IP             AP Profile
-------------------------------------------------------------------------------------------
APe865.49d9.bfe0        e865.49ea.a4b0    WSM2+Ant    198.51.100.2        house24

APa89d.21b9.69d0        a89d.21b9.69d0    Local       198.51.100.3        house24

APe4aa.5d3f.d750        e4aa.5d5f.3630    WSM         198.51.100.4        house24
```

To display the overall (profile specific) configuration values and operational status for a given profile, use the following command:

```
Device# show ap profile profile-name hyperlocation summary

Profile Name: profile-name
Hyperlocation operational status: Up
   Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -100
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

To display both the overall (profile specific) and per-AP configuration values and operational status for a given profile, use the following command. The APs listed are only those APs that belong to the specified join profile.

```
Device# show ap profile profile-name hyperlocation detail

Profile Name: profile-name
Hyperlocation operational status: Up
 Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7

AP Name                 Radio MAC         Method      CMX IP
-----------------------------------------------------------------
APf07f.0635.2d40        f07f.0635.2d40    WSM2+Ant    198.51.100.2
APf07f.0635.2d41        f07f.0635.2d41    Local       198.51.100.3
APf07f.0635.2d42        f07f.0635.2d42    WSM         198.51.100.4
```

To display configuration values for an AP profile, use the following command:

```
Device# show ap profile profile-name detailed

Hyperlocation :
  Admin State             : ENABLED
  PAK RSSI Threshold Detection: -100
  PAK RSSI Threshold Trigger  : 10
  PAK RSSI Threshold Reset    : 8
.
.
.
```

To display the Cisco CMXs that are correctly joined and used by hyperlocation, use the following command:

```
Device# show ap hyperlocation cmx summary

Hyperlocation-enabled CMXs

IP            Port Dest MAC        Egress src MAC Egress VLAN Ingress src MAC Join time

-------------------------------------------------------------------------------------------------
198.51.100.4  2003 aaaa.bbbb.cccc  aabb.ccdd.eeff 2           0000.0001.0001  12/14/18
09:27:14
```

To display the hyperlocation client statistics, use the following command:

```
Device# show platform hardware chassis active qfp
feature wireless wlclient cpp-client summary

Client Type Abbreviations:
  RG - REGULAR BL - BLE
  HL - HALO    LI - LWFL INT
Auth State Abbreviations:
  UK - UNKNOWN IP - LEARN IP IV - INVALID
  L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
  UK - UNKNOWN IN - INIT
  LC - LOCAL   AN - ANCHOR
  FR - FOREIGN MT - MTE
  IV - INVALID
EoGRE Abbreviations:
  N - NON EOGRE Y - EOGRE
 CPP IF_H     DPIDX      MAC Address    VLAN  CT  MCVL  AS  MS  E  WLAN POA
------------------------------------------------------------------------------
   0X32     0XF0000001  0000.0001.0001   9    HL   0    RN  LC  N       NULL
```

To display the interface handle value statistics, use the following command:

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0x32 statistics start
```

To display the recorded flow, use the following command:

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0X32 statistics

                  Pkts               Bytes
Rx                 26                3628
```

To stop statistics capture, use the following command:

```
Device# show platform hardware chassis active
qfp feature wireless wlclient datapath cpp-if-handle 0x32 statistics stop
```

To view the APs requested by Cisco CMX with AP groups' support, use the following commands:

```
Device# show nmsp subscription group summary

CMX IP address: 198.51.100.4
  Groups subscribed by this CMX server:
  Group name: CMX_1198.51.100.4

Device# show nmsp subscription group detail ap-list CMX_198.51.100.1 198.51.100.1

CMX IP address: 198.51.100.1
CMX Group name: CMX_198.51.100.1
CMX Group AP MACs:
: aa:bb:cc:dd:ee:01 aa:bb:cc:dd:ee:02 aa:bb:cc:dd:ee:03 aa:bb:cc:dd:ee:03
```

To display the NTP IP address and authentication parameters, use the following command:

```
Device# show ap profile profile-name detailed
.
.
.
NTP Authentication : ENABLED
Key id : 2
Key type : SHA1
Key format : HEX
Key : 3a2275c74c250c362ca63e4af06fa3f3cd8d4aec
Encryption type : Clear

.
.
.
```

To display the NTP status for each AP, use the following command:

```
Device# show ap name AP-G1-230 ntp status

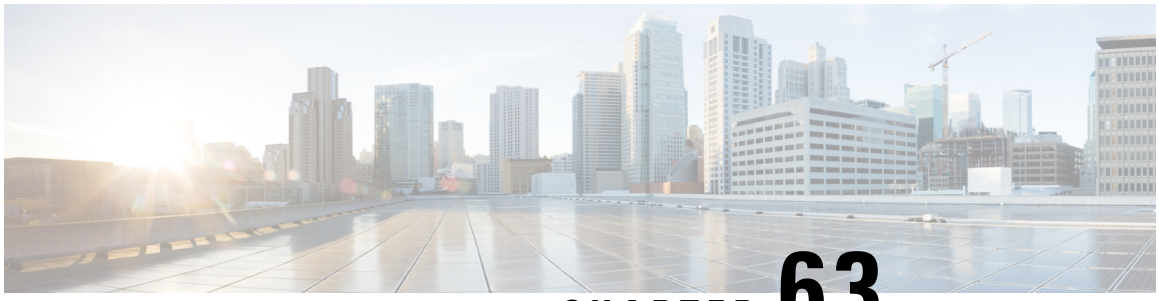
ap-name       enabled v4/v6 IPAddress       Status     Stratum LastSync  SyncOffset
AP-G1-230     Y       v4    198.51.100.5    AuthFail   4       1000      100
```

To display NTP status for all the APs, use the following command:

```
Device# show ap ntp status

ap-name       enabled v4/v6 IPAddress  Status  Stratum LastSync  SyncOffset
AP-G1-230         Y      v4   5.5.5.5  AuthFail 2        Never
AP-G1-231         Y      v4   5.5.5.10  Synced  3        1000       100
AP-G1-232         Y      v4   5.5.5.15  Synced  16       2000        50
```

To display the instant status of NTP synchronization in an AP, use the following command. The following output is from an AP and not from the controller.

```
Device# show ntp
```

```
!This error message is displayed when NTP is not configured.
%Error: ntpd is not running

!The following output is displayed when NTP is configured.
Stratum  Version  Last Received    Delay     Offset    Jitter   NTP server
13       4        7sec ago         1.124ms   0.536ms   0.001ms  198.51.100.5
```

To display AP timezone information, use the following command:

```
Device# show ap timezone

AP Name   Status   Offsets(h/m)
--------------------------
AP1       Disabled    0:0
AP2       Enabled     1:0
```

Verifying Hyperlocation BLE Beacon Configuration

To verify the list of configured BLE beacons, use the following command:

```
Device# show ap profile ap-profile-name hyperlocation ble-beacon
BLE Beacon interval (Hz): 1
BLE Beacon advertised attenuation value (dBm): -59

ID              UUID                 TX Power(dBm) Status
-----------------------------------------------------------------
0 ffffffff-aaaa-aaaa-aaaa-aaaaaaaaaaaa 0 Enabled
1 ffffffff-bbbb-bbbb-bbbb-bbbbbbbbbbbb 0 Enabled
2 ffffffff-gggg-gggg-gggg-gggggggggggg 0 Enabled
3 ffffffff-dddd-dddd-dddd-dddddddddddd 0 Enabled
4 ffffffff-eeee-eeee-eeee-eeeeeeeeeeee 0 Enabled
```

Verifying Hyperlocation BLE Beacon Configuration for AP

To verify the Hyperlocation BLE Beacon configuration for an AP, use the following command:

```
Device# show ap name test-ap hyperlocation ble-beacon
BLE Beacon interval (Hz): 1
BLE Beacon advertised attenuation value (dBm): -60

ID Status UUID Major Minor TXPower(dBm)
-------------------------------------------------------------------------------
0 Enabled 99999999-9999-9999-9999-999999999999 8 0 -0
1 Enabled bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb 8 1 -0
2 Enabled 88888888-8888-8888-8888-888888888888 8 2 -0
3 Enabled dddddddd-dddd-dddd-dddd-dddddddddddd 8 3 -0
4 Enabled eeeeeeee-eeee-eeee-eeee-eeeeeeeeeeee 8 4 -0
```



CHAPTER 63

FastLocate for Cisco Catalyst Series Access Points

- Information About FastLocate, on page 755
- Restrictions on FastLocate, on page 755
- Supported Access Points, on page 756
- FastLocate Network Components, on page 756
- Configuring FastLocate (GUI), on page 757
- Verifying FastLocate on Cisco Catalyst APs, on page 757

Information About FastLocate

Current Wi-Fi location technology relies on mobile devices sending received signal strength indication (RSSI) or location information, based on probe request messaging, to access points. This information is sent on most channels by the mobile device and received by neighbor APs on different channels. This helps in location estimation.

Wi-Fi clients are moving towards lesser probing to discover an AP. This helps to conserve battery power. Depending on the client, operating system, driver, battery, current, and client activity, device probing frequency varies anywhere from 10 seconds to 5 minutes. This variation results in inadequate data points to represent real-world movement.

Since data packets are more frequent than probe request packets, they can be aggregated better. FastLocate enables higher location refresh rates by collecting RSSI or location information through data packets received by the APs. Using these data packets, location- based services (LBS) updates are initiated by the network and are available more frequently.

Restrictions on FastLocate

In Fabric deployments, the Wireless Management Interface (WMI) cannot be an L3 interface (Loopback Interface).

Note It is recommended to use a VLAN interface as the WMI, if you want to use FastLocate in Fabric deployment.

Supported Access Points

Beginning with IOS XE 17.1.1, FastLocate feature is supported on the Cisco Catalyst 9120 Series Access Points.

In IOS XE 17.3.1, the following APs support the FastLocate feature:

- Cisco Catalyst 9130 Series Access Points
- Cisco Catalyst 9120 Series Access Points
- Cisco Aironet 4800 Series Access Points.
- Cisco Aironet 3800 Series Access Points.
- Cisco Aironet 2800 Series Access Points.

In addition, Cisco Aironet 4800 Series Access Points also supports the Angle of Arrival based location calculation (Hyperlocation).

When FastLocate is enabled, the Cisco RF ASIC radios of these APs act as a WSSI module and transform into a monitoring role and off-channel scanning mode. The Cisco RF ASIC radios scan through all the 2.4-GHz channels and 5-GHz channels in a linear fashion, with each channel scanned for 150 milliseconds. This period is called the dwell time.

The Cisco RF ASIC radios of the APs are synchronized with the NTP server. Using FastPath, all data packet RSSI records that are collected during one off-channel dwell is sent in a specific packet format to the Cisco controller, at the end of the dwell time.

FastLocate Network Components

For successful packet RSSI location computation, the following components with necessary functionalities are needed:

- Wireless client
  - Send data, management, and control packets
- Cisco Catalyst 9800 Series Wireless Controller
  - Configure NTP server information and location parameters on AP
  - Forward clients' RSSI related information to CMX/MSE via FastPath/datapath
- Cisco Catalyst 9120 Series AP
  - Location radio in monitor or equivalent role
  - Time synchronized with NTP server
  - Collect RSSI related data sent by clients (both associated and unassociated)
  - Send clients' RSSI data to the Cisco controller through CAPWAP
- Cisco CMX

- Parse fastpath location data received by WLC
- Calculate exact physical location of the client and render on GUI using algorithms

Configuring FastLocate (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join** page, click the **default-ap-profile** AP join profile.

Step 3 In the **Edit AP Join Profile** window, click the **AP** tab.

Step 4 Under **Hyperlocation**, select the **Enable Hyperlocation** check box.

Step 5 Click **Update & Apply to Device**.

Verifying FastLocate on Cisco Catalyst APs

To verify FastLocate, use the below commands on the AP:

```
Device# show ntp

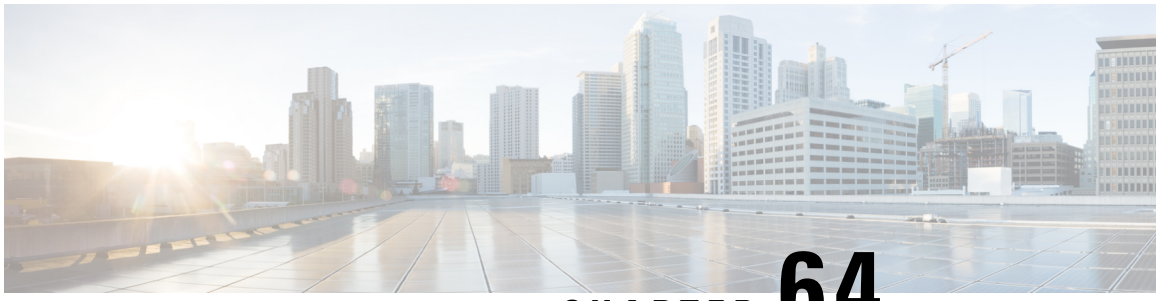
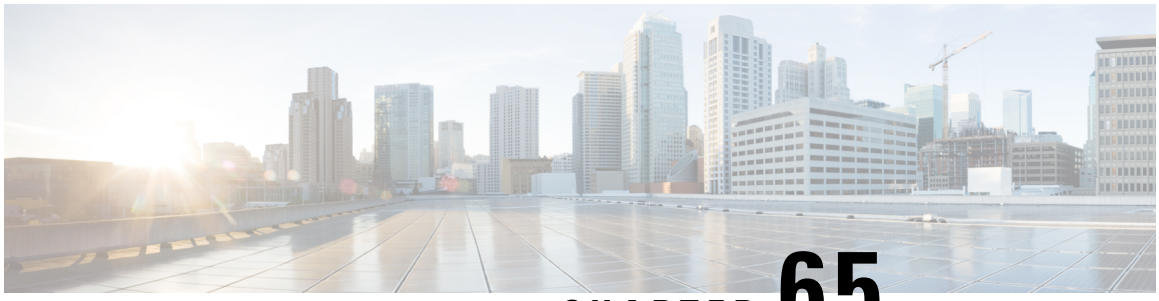
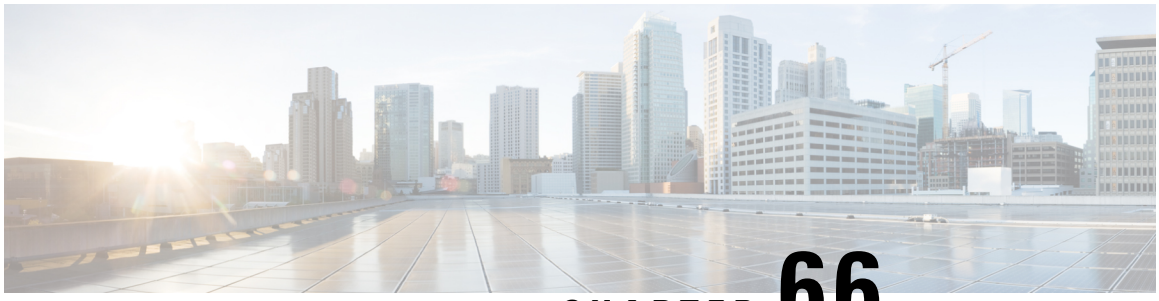
Stratum   Version   Last Received   Delay    Offset    Jitter    NTP server
   1         4         123sec ago   1.169ms  -3.262ms  10.050ms    7.7.7.2

Device# show ap fast-path statistics

total packets sent   : 90001
invalid app ID drops : 0
application                  : 0 (HALO)
packets sent (CAPWAP)        : 90001
packets sent (APP HOST INTF) : 0
admin state drops            : 0
no dest IP drops             : 0
```

To view FastLocate admin status details on the AP, use the following command:

```
Device# show capwap client rcb

Hyperlocation Admin State    : Enabled
MSE Gateway MAC              : 00:50:56:86:0F:9D
WLC Hyperlocation Source Port: 9999
MSE IP Address               : 10.0.0.1
```

To view FastPath-related parameters on the AP like source and destination IP addresses, port numbers, and the gateway MAC address, use the following command:

```
Device# show ap fast-path configuration hyperlocation

source IP address     : 10.0.0.2
destination IP address: 10.0.0.1
```

```
source port (WLC)     : 9999
destination port (MSE): 2003
gateway MAC           : 00:50:56:86:0F:9D
ewlc hyperlocation MAC: 00:00:00:01:00:01
```

To verify FastLocate on the Cisco Catalyst controller, use the appropriate command given below.

To view the summary of applications that send fastpath or datapath data, use the below command. The hexcode for the HyperLocation and BLE port numbers are displayed.

```
Device# show platform hardware chassis active qfp feature wireless wlclient
 cpp-client summary


Client Type Abbreviations:
RG - REGULAR     BL - BLE
HL - HALO        LI - LWFL INT
Auth State Abbreviations:
UK - UNKNOWN     IP - LEARN IP    IV - INVALID
L3 - L3 AUTH     RN - RUN
Mobility State Abbreviations:
UK - UNKNOWN     IN - INIT
LC - LOCAL       AN - ANCHOR
FR - FOREIGN     MT - MTE
IV - INVALID
EoGRE Abbreviations:
N - NON EOGRE    Y - EOGRE
CPP IF_H    DPIDX        MAC Address VLAN CT MCVL AS MS E WLAN POA
------------------------------------------------------------------------
0X31   0XF0000002 0000.0003.0001 122 BL 0 RN LC N NULL 0X32 0XF0000001 0000.0001.0001 122
HL 0 RN LC N NULL
```

To capture statistics of a selected application, use the below command:

```
Device# show platform hardware chassis active qfp feature wireless wlclient
 datapath
cpp-if-handle register-code statistics start
```

The hex-value of the register-code is obtained from the **show platform hardware chassis active qfp feature wireless wlclient cpp-client summary** command mentioned earlier.

```
Device# show platform hardware chassis active qfp feature wireless wlclient
 datapath cpp-if-handle 0x32 statistics start
```

To display the statistics of the selected application, use the below command:

```
Device# show platform hardware chassis active qfp feature wireless wlclient
 datapath
cpp-if-handle register-code statistics
```

The hex-value of the register-code is obtained from the **show platform hardware chassis active qfp feature wireless wlclient cpp-client summary** command mentioned earlier.

```
Device# show platform hardware chassis active qfp feature wireless wlclient
 datapath cpp-if-handle 0x32 statistics
    Pkts   Bytes
Rx   232   38850
```



CHAPTER 64

IoT Services Management

- Information About IoT Services Management, on page 759
- Enabling the Dot15 Radio, on page 760
- Configuring the gRPC Token, on page 760
- Enabling gRPC in an AP Profile, on page 761
- Verifying BLE State and Mode, on page 761
- Verifying BLE Details, on page 762
- Verifying gRPC Summary, Status, and Statistics, on page 763

Information About IoT Services Management

Cisco Catalyst 9800 devices running the Cisco IOS-XE image Version 17.3.2 support Cisco Spaces: IoT Services along with the Network Assurance on Cisco Catalyst Center. However, IoT Services and the Intelligent Capture (iCAP) port configuration are mutually exclusive. That is, if the iCAP feature needs to be enabled on a device, then IoT Services cannot be deployed. Similarly, if IoT Services needs to be enabled on a device, then iCAP feature cannot be deployed.

The following are the gRPC connections from AP:

- One gRPC connection from AP to Cisco Catalyst Center for iCAP.
- Other gRPC connection from AP to Cisco Catalyst Center Connector for IoT Services.

Following is a table that shows the pairs of configurations that can or cannot coexist on IOS-XE image version 17.3.2.

Cisco DNA-C Configuration	Cisco Spaces Configuration	Coexistence on IOS-XE Image Version 17.3.2
network-assurance enable	**ap cisco-dna token** *token*	yes
network-assurance icap server port *port*	**ap cisco-dna token** *token*	no

Cisco Spaces: IoT Services is an end-to-end solution. Hence, you do not need to manually enable IoT services or Dot15 radio on the controller. Dot15 radio is enabled or disabled automatically through Cisco Spaces. However, you can verify if Dot15 radio is enabled from the controller.

Similarly, Cisco Spaces enables gRPC in the **default ap profile configuration** of the controller. You do not need to manually enable it. However, you can verify the same on the controller.

Cisco Spaces enables the **apphost** configuration, which is required for the **default ap profile** configuration. If **apphost** is not enabled by Cisco Spaces, then you must manually enable it. This is required in order to host IOx applications on an AP.

Enabling the Dot15 Radio

When you enable the BLE radio configuration globally, the APs that are joined to the controller enable their BLE radio, if they have the BLE radio chip in their hardware. This configuration will be applied to all the APs that will join the controller after the configuration is enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no ap dot15 shutdown** **Example:** `Device(config)# no ap dot15 shutdown`	Enables the dot15 radios for APs, globally.
Step 3	**ap dot15 shutdown** **Example:** `Device(config)# ap dot15 shutdown`	Disables the dot15 radio for all APs, globally.

Configuring the gRPC Token

Note

- The configuration is pushed automatically from Cisco Spaces. There is no need to manually enable gRPC on the **default ap profile** configuration. You can verify the same on the controller
- The NETCONF (NETCONF/YANG configuration) must be enabled on the device for the Cisco Spaces to push the required configuration to the controller. Secure Copy (**ip scp server enable**) must be enabled on the controller so that Cisco Spaces can push the gRPC certificate to the controller.
- The iCAP server port configuration should not be present in the configuration. If it exists, then run the iCAP server port 0 command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**ap cisco-dna token** {**0** | **8**} *cisco-token-number* **Example:** `Device(config)# ap cisco-dna token 0 cisco-token-number`	Configures the Cisco Spaces gRPC token. **0**: Specifies the string as an UNENCRYPTED password. **8**: Indicates the placeholder for backward compatibility.

Enabling gRPC in an AP Profile

The Manage Streams feature of Cisco Spaces pushes the gRPC configuration only to the default AP profile, currently. If you are using a different AP profile, you must manually configure gRPC.

The following procedure explains how to manually enable gRPC on an AP profile that is not the default-ap-profile. Cisco Spaces may not push gRPC on all the AP profiles. Therefore, the following commands can be used to enable gRPC for individual AP profiles.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures the AP profile and enters the AP profile configuration mode.
Step 3	**cisco-dna grpc** **Example:** `Device(config-ap-profile)# cisco-dna grpc`	Enables the gRPC channel on the APs, in the AP profile.

Verifying BLE State and Mode

To verify the BLE state and mode, run the following command:

```
Device# show ap ble summary
AP Name         BLE AP State         BLE mode
-------------------------------------------------------------------------
Axel-1           Up                  Advanced (IOx)
Axel-2           Up                  Advanced (IOx)
9117-1           Up                  Advanced (IOx)
3800-1           Up                  Base (Native)
1815             Up                  Base (Native)
9120-3           Up                  Advanced (IOx)
```

```
9120-1          Up                Base (Native)
9115-ax         Up                Base (Native)
9120-2          Up                Base (Native)
```

Verifying BLE Details

To verify BLE details, run the following command:

```
Device# show ap name APXXXX.BDXX.29XX ble detail
Mode report time          : 07/28/2020 09:40:57
Mode                      : Base (Native)
Radio mode                : BLE
Admin state report time   : 07/28/2020 09:40:57
Admin state               : Up
Interface report time     : 07/28/2020 09:40:57
Interface                 : MSM1
Interface state           : Open
Type                      : Integrated
Capability report time    : 07/14/2020 17:10:49
Capability                : BLE, Zigbee, USB,
Host data report time     : 07/28/2020 09:52:04
Host data
  Device name                : APXXXXBDX
  Dot15 Radio MAC            : 18:04:ed:c5:0e:c8
  API version                : 1
  FW version                 : 2.7.16
  Broadcast count            : 4389
  Uptime                     : 596050 deciseconds
  Active profile             : viBeacon
Scan Statistics report time    : 07/28/2020 09:40:57
Scan statistics
  Total scan records         : 0
Scan role report time  : 07/28/2020 09:43:19
Scan role
  Scan state                 : Disable
  Scan interval              : 0 seconds
  Scan window                : 800 milliseconds
  Scan max value             : 8
  Scan filter                : Enable
Broadcaster role
  Current profile type: iBeacon
  Last report time           : N/A
    UUID                     : Unknown
    Major                    : Unknown
    Minor                    : Unknown
    Transmit power           : Unknown
    Frequency                : Unknown
    Advertised transmit power : Unknown
  Current profile type: Eddystone URL
  Last report time           : 07/28/2020 09:47:17
    URL                      : https://www.cisco.com
  Current profile type: Eddystone UID
  Last report time           : 07/28/2020 09:43:25
    Namespace                : 04d77XXXXXXXXXXXXXX
    Instance id              : 5df5XXXXXXXX
  Current profile type: viBeacon
  Last report time           : 07/28/2020 09:52:04
    Interval                 : 450 milliseconds
    Beacon ID                : 0
      UUID                      : 30XXXXXX-3XXX-4XXX-9XXX-d3XXXXXXXXXX
      Major                     : 36341
      Minor                     : 33196
```

```
  Transmit power             : 3 dBm
  Advertised transmit power  : 60 dBm
  Enable                     : Enable
Beacon ID                 : 1
  UUID                       : 57XXXXXX-cXXX-4XXX-aXXX-85XXXXXXXXXX
  Major                      : 3875
  Minor                      : 567
  Transmit power             : 2 dBm
  Advertised transmit power  : 69 dBm
  Enable                     : Enable
.
.
.
```

Verifying gRPC Summary, Status, and Statistics

To verify the gRPC summary, run the following command:

```
Device# show ap grpc summary
AP Name              AP Mac             gRPC Status
-------------------------------------------------------------------------------
APXXXX.BDXX.F2XX     0cXX.bdXX.66XX     Up
```

To verify the packet statistics on the gRPC channel that also shows the transmit and receive failures, run the following command:

```
Device# show ap name APXXXX.BDXX.F2XX grpc detail
gRPC channel status : Up
Packets transmit attempts : 62
Packets transmit failures : 0
Packets receive count : 62
Packets receive failures : 0
```



CHAPTER 65

IoT Module Management in the Controller

- Information About IoT Module Management in the Controller, on page 765
- Enabling a USB on the Controller, on page 765
- Verifying the USB Modules, on page 766

Information About IoT Module Management in the Controller

The IoT Module Management feature uses the USB interface on the Cisco Catalyst 9105AXI, 9105AXW, 9115AX, 9117AX, 9120AX, and 9130AX Series access points (APs), to connect to the Cisco Internet of Things (IoT) connector. These APs host the third-party application software components, that act as containers. Cisco Catalyst Center helps in the provisioning, deployment, and life cycle management of the container applications on the APs. The controller and the APs are managed by Cisco Catalyst Center.

You can connect the USB modules to the APs, and then log in to the controller and run commands to enable the USB modules and the Cisco IOx application in the APs associated with an AP profile group.

Enabling a USB on the Controller

To enable a USB for all the APs connected in an AP profile and to enable Cisco IOx on all the APs, follow this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap profile name* **Example:** `Device(config)# ap profile ap-profile-test`	Configures an AP profile and enters AP profile configuration mode. **Note** You can use the default AP profile (default-ap-profile) or create a named AP profile, as shown in the example in the adjacent column.

	Command or Action	Purpose
Step 3	**apphost** **Example:** `Device(config-ap-profile)# apphost`	Enables the apphost framework on Cisco APs.
Step 4	**usb-enable** **Example:** `Device(config-ap-profile)# usb-enable`	Enables a USB for Cisco APs.
Step 5	**exit** **Example:** `Device(config-ap-profile)# exit`	Exits AP profile configuration mode.
Step 6	**copy running-config startup-config** **Example:** `Device(config)# copy running-config startup-config`	Writes running configuration to the memory.

Verifying the USB Modules

To verify the state of USB modules, run the following command:

```
Device# show ap config general
USB Module Type            : USB Module
USB Module State           : Enabled
USB Operational State      : Enabled
USB Override               : Disabled
```

To verify the apphost status, run the following command:

```
Device# show ap apphost summary
AP Name                 AP Mac               Apphost Status           CAF Port
Apphost HW capable
-----------------------------------------------------------------------------------------------------
SS-2027                 00xx.abXX.bXXX       Up                       8443             Yes
Axel-2036               04xx.40XX.aXXX       Up                       8443             Yes
Haida-PrePilot          0cxx.f8XX.0XXX       Up                       8443             Yes
Somer-infra-2022        3cxx.0eXX.0XXX       Up                       8443             Yes
AP5C71.0DEC.DB5C        3cxx.0eXX.0XXX       Up                       8443             Yes
AP5C71.0DEC.E3D8        3cxx.0eXX.4XXX       Up                       8443             Yes
Somer-WP-2021           3cxx.0eXX.5XXX       Up                       8443             Yes
AP5C71.0DEC.EC60        3cxx.0eXX.9XXX       Up                       8443             Yes
SS-2005                 6cXX.05XX.dXXX       Up                       8443             Yes
Vanc-2042               d4XX.bdXX.2XXX       Up                       8443             Yes
```

To verify the apphost status, run the following command:

```
Device# show ap module summary
AP Name         External Module       External Module PID  External Module Description
-----------------------------------------------------------------------------------------
Axel-2036       Enable 10xx/eaXX/100  CP2XXXX              USB to UART Bridge C
Haxx-PrePilot   Enable 10xx/eaXX/100  CP2XXXX              USB to UART Bridge C
APXXX.0XXX.EXX  Enable 10xx/eaXX/100  CP2XXXX              USB to UART Bridge C
SS-2005         Enable 10xx/eaXX/100  CP2XXXX              USB to UART Bridge C
Vaxx-2006       Enable 10xx/eaXX/100  CP2XXXX              USB to UART Bridge C
```



CHAPTER 66

Cisco Spaces

- Cisco Spaces, on page 767
- Configuring Cisco Spaces, on page 767
- Verifying Cisco Spaces Configuration, on page 768

Cisco Spaces

Cisco Spaces is the next generation indoor location services platform. The Network Mobility Services Protocol (NMSP) cloud-service of the wireless controller communicates with Cisco Spaces using HTTPS as a transport protocol.

Configuring Cisco Spaces

Follow the procedure given below to configure Cisco Spaces:

Before you begin

- **Configure DNS**—To resolve fully qualified domain names used by NMSP cloud-services, configure a **DNS** using the **ip name-server** *server_address* configuration command as shown in Step 2.
- **Import 3rd party root CAs**—The controller verifies the peer and the host based on the certificate that is sent by the CMX when a connection is established. However, root CAs are not preinstalled on the controller. You have to import a set of root CAs trusted by Cisco to the trustpool of the crypto PKI by using the **crypto pki trustpool import url <url>** configuration command as shown in Step 3.
- A successful registration to Cisco Spaces is required to enable **server url** and **server token** parameters configuration which is needed to complete this setup.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ip name-server** *namesvr-ip-addr* **Example:** `Device(config)#ip name-server 10.10.10.205`	Configures the DNS on the controller to resolve the FQDN names used by the NMSP cloud-services.
Step 3	**crypto pki trustpool import url** *url* **Example:** `Device(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	Imports the 3rd party root CA. The controller verifies the peer using the imported certificate.
Step 4	**[no] nmsp cloud-services server url** *url* **Example:** `Device(config)# nmsp cloud-services server url https://cisco.com`	Configures the URL used for cloud services. Use the **no** form of the command to delete the server url from the configuration.
Step 5	**[no] nmsp cloud-services server token** *token* **Example:** `Device(config)# nmsp cloud-services server token test`	Configures the authentication token for the NMSP cloud service. Use the **no** form of the command to delete the server token from the configuration.
Step 6	**[no] nmsp cloud-services http-proxy** *proxy-server port* **Example:** `Device(config)# nmsp cloud-services http-proxy 10.0.0.1 10`	(Optional) Configures HTTP proxy details for the NMSP cloud service. Use the **no** form of the command to disable the use of a HTTP proxy.
Step 7	**[no] nmsp cloud-services enable** **Example:** `Device(config)# nmsp cloud-services enable`	Enables NMSP cloud services. Use the **no** form of the command to disable the feature.

Verifying Cisco Spaces Configuration

Use the following commands to verify the Cisco Spaces configuration.

To view the status of active NMSP connections, use the following command:

```
Device# show nmsp status

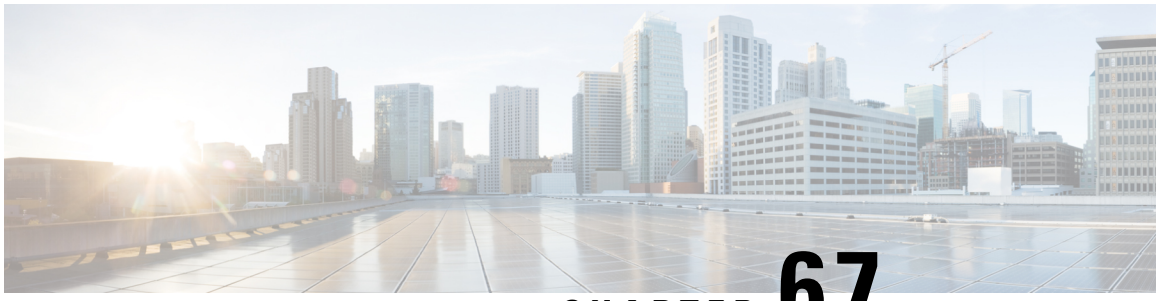
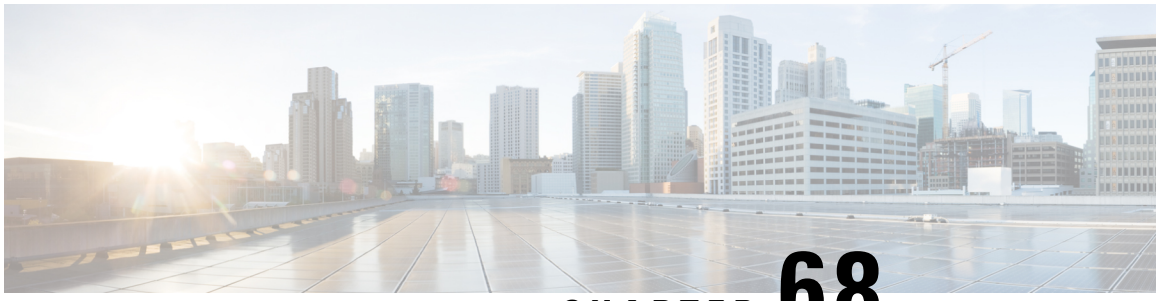
MSE IP Address   Tx Echo Resp  Rx Echo Req   Tx Data     Rx Data   Transport
------------------------------------------------------------------------------
9.9.71.78        0             0             1           1         TLS
64.103.36.133    0             0             1230        2391      HTTPs
```

To view the NMSP cloud service status, use the following command:

```
Device# show nmsp cloud-services summary

CMX Cloud-Services Status
```

```
------------------------

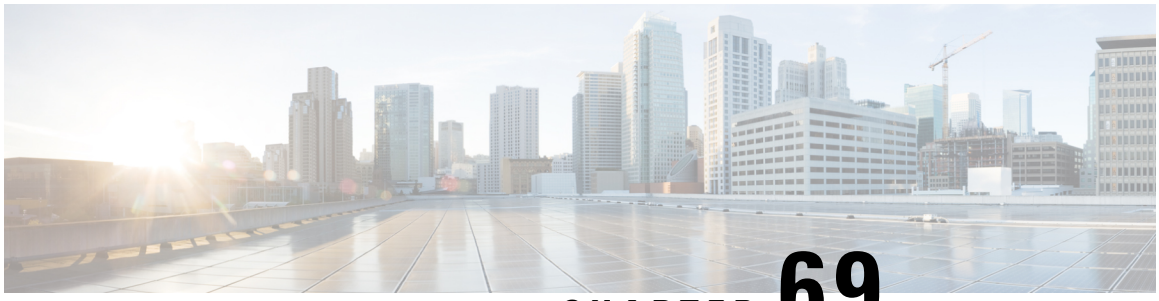
   Server:                                 https://yenth8.cmxcisco.com
   IP Address:                             64.103.36.133
   Cmx Service:                            Enabled
   Connectivity:                           https: UP
   Service Status:                         Active
   Last Request Status:                    HTTP/1.1 200 OK
   Heartbeat Status:                       OK
```

To view the NMSP cloud service statistics, use the following command:

```
Device# show nmsp cloud-services statistics

CMX Cloud-Services Statistics
-----------------------------

   Tx DataFrames:                           3213
   Rx DataFrames:                           1606
   Tx HeartBeat Req:                       31785
   Heartbeat Timeout:                          0
   Rx Subscr Req:                           2868
   Tx DataBytes:                           10069
   Rx DataBytes:                           37752
   Tx HeartBeat Fail:                          2
   Tx Data Fail:                               0
   Tx Conn Fail:                               0
```

To view the mobility services summary, use the following command:

```
Device# show nmsp subscription summary

Mobility Services Subscribed:
Index Server IP Services
----- --------- --------
1 209.165.200.225 RSSI, Info, Statistics, AP Monitor, AP Info
2 209.165.200.225 RSSI, Statistics, AP Info
```



CHAPTER 67

EDCA Parameters

- Enhanced Distributed Channel Access Parameters, on page 771
- Configuring EDCA Parameters (GUI), on page 771
- Configuring EDCA Parameters (CLI), on page 772

Enhanced Distributed Channel Access Parameters

Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

This section contains the following subsections:

Configuring EDCA Parameters (GUI)

Procedure

Step 1 Choose **Configuration > Radio Configurations > Parameters**. Using this page, you can configure global parameters for 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz) radios.

Note You cannot configure or modify parameters, if the radio network is enabled. Disable the network status on the Configuration > Radio Configurations > Network page before you proceed.

Step 2 In the **EDCA Parameters** section, choose an EDCA profile from the **EDCA Profile** drop-down list. Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

Step 3 For 802.11a/n/ac (5 GHZ) radios, in the (DFS 802.11h) section, enter the local power constraint. You cannot configure power constraint if the DTPC Support check box on the **Configure > Radio Configurations > Network** page is checked. The valid range is between 0 dBm and 30 dBm.

Step 4 Check the **Channel Switch Announcement Mode** check box, if you want the AP to announce when it is switching to a new channel and the new channel number. The default value is disabled.

Step 5 Check the **Smart DFS** check box to enable Dynamic Frequency Selection (DFS) and avoid interference with the radar signals.

Step 6 Click **Apply**.

Configuring EDCA Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz | 24ghz | 6ghz} shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the radio network.
Step 3	**ap dot11 {5ghz | 24ghz | 6ghz} edca-parameters {client-load-based | custom-voice | fastlane | optimized-video-voice | optimized-voice | svp-voice | wmm-default}** **Example:** `Device(config)# ap dot11 5ghz edca-parameters optimized-voice`	Enables specific EDCA parameters for the 802.11a, 802.11b/g, or 802.11 6-GHz network. **Note** The **custom-voice** option is not supported for Cisco Catalyst 9800 Series Wireless Controller. • **client-load-based**: Enables client load based EDCA configuration. • **custom-voice**: Enables custom voice parameters for the 802.11a or 802.11b/g network. • **fastlane**: Enables the fastlane parameters for the 802.11a or 802.11b/g network. • **optimized-video-voice**: Enables EDCA voice-optimized and video-optimized parameters for the 802.11a or 802.11b/g network. Choose this option when both voice and video services are deployed on your network. • **optimized-voice**: Enables non-SpectraLink voice-optimized profile parameters for the 802.11a or 802.11b/g network. Choose this option when voice services other than SpectraLink are deployed on your network. • **svp-voice**: Enables SpectraLink voice-priority parameters for the 802.11a or 802.11b/g network. Choose this option if SpectraLink phones are deployed on

	Command or Action	Purpose
		your network to improve the quality of calls. • **wmm-default**: Enables the Wi-Fi Multimedia (WMM) default parameters for the 802.11a or 802.11b/g network. This is the default option. Choose this option when voice or video services are not deployed on your network.
Step 4	**no ap dot11 {5ghz | 24ghz | 6ghz} shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Enables the radio network.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**show ap dot11 {5ghz | 24ghz | 6ghz} network** **Example:** `Device# show ap dot11 5ghz network`	Displays the current status of MAC optimization for voice.



CHAPTER 68

Adaptive Client Load-Based EDCA

- Feature History for Adaptive Client Load-Based EDCA, on page 775
- Information About Adaptive Client Load-Based EDCA, on page 775
- Restrictions for Adaptive Client Load-Based EDCA, on page 776
- Configuration Workflow, on page 776
- Configuring Adaptive Client Load-Based EDCA (GUI), on page 776
- Configuring Adaptive Client Load-Based EDCA (CLI), on page 777
- Verifying Adaptive Client Load-Based EDCA Configuration, on page 777

Feature History for Adaptive Client Load-Based EDCA

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 55: Feature History for Adaptive Client Load-Based EDCA

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.5.1	Adaptive Client Load-Based EDCA	This Adaptive Client Load-Based EDCA feature dynamically changes Enhanced Distributed Channel Access (EDCA) parameters of clients based on the active client and load that significantly reduce collisions.

Information About Adaptive Client Load-Based EDCA

The static EDCA configuration is good for small number of clients. In an enterprise multiclient deployment scenario, access points (APs) experience excessive collisions as the number of clients increases resulting in significant performance degradation. To overcome such a scenario, the Adaptive Client Load-Based EDCA feature has been introduced.

This feature dynamically changes EDCA parameters of clients based on the active client and load that significantly reduce collisions.

Feature Scenario

Run-time EDCA configuration based on active clients and load.

Use Case

In a dense multiclient deployment scenario, when a customer was testing 40 iPads in a class room or auditorium setup, he observed that the channel utilization was 60 to 70 percent. The overall AP throughput was less because of air collusion and RTS retries.

After the adaptive client load-based EDCA feature was enabled, the overall throughput increased by 15 to 20 percent and collision decreased by 30 to 40 percent.

Restrictions for Adaptive Client Load-Based EDCA

- You must disable the 802.11b network if you want to access the 802.11a network.

Configuration Workflow

- Configuring Adaptive Client Load-Based EDCA (GUI)
- Configuring Adaptive Client Load-Based EDCA (CLI)

Configuring Adaptive Client Load-Based EDCA (GUI)

Procedure

Step 1 Choose **Configuration > Radio Configurations > Parameters** to configure global parameters for 802.11a/n/ac (5-GHz) and 802.11b/g/n (2.4-GHz) radios.

Step 2 In the **EDCA Parameters** section, from the **EDCA Profile** drop-down list, choose an EDCA profile.

Step 3 Click the **Client Load Based Configuration** toggle button to enable or disable. It is enabled by default.

Step 4 For 802.11a/n/ac (5-GHz) radios, in the **DFS (802.11h)** section, enter the local power constraint. You cannot configure power constraint if the **DPTC Support** check box in **Configuration > Radio Configurations > Network** is checked. The valid range for power constraint is between 0 dBm and 30 dBm.

Step 5 From the **Channel Switch Announcement Mode** drop-down list, choose either the **Loud** or **Quiet** mode.

Step 6 Click the **Smart DFS** toggle button to enable or disable. It is enabled by default.

Step 7 In the **11ax Parameters** section, enable or disable the following, using the corresponding toggle button:

- **Target Wakeup Time**
- **Target Wakeup Time Broadcast**
- **Multiple Bssid**

Step 8 Enable BSS color globally for the 5-GHz and 2.4-GHz radios by checking the **BSS Color** check box.

Step 9 Click **Apply**.

Configuring Adaptive Client Load-Based EDCA (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **edca-parameters client-load-based** **Example:** `Device(config)# ap dot11 24ghz edca-parameters client-load-based`	Enables client load-based EDCA configuration for 802.11 radios. Use the **no** form of this command to disable the configuration. **Note** To enable the configuration on an 802.11a radio, you must disable the 802.11b network.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying Adaptive Client Load-Based EDCA Configuration

To verify whether the Adaptive Client Load-Based EDCA feature is enabled on an 802.11a or an 802.11b radio, use the following command:

```
Device# show ap dot11 24ghz network
Device# show ap dot11 5ghz network
EDCA profile type check                  : default-wmm
Client Load Based EDCA Config            : Enabled
```

To verify whether the Adaptive Client Load-Based EDCA feature is enabled on an 802.11 6-GHz radio, use the following command:

```
Device# show ap dot11 6ghz network
.
.
.
EDCA profile type check                  : default-wmm
Client Load Based EDCA Config            : Enabled
```

To verify whether the Adaptive Client Load-Based EDCA feature is enabled on APs, use the following command:

```
Device# show capwap client config

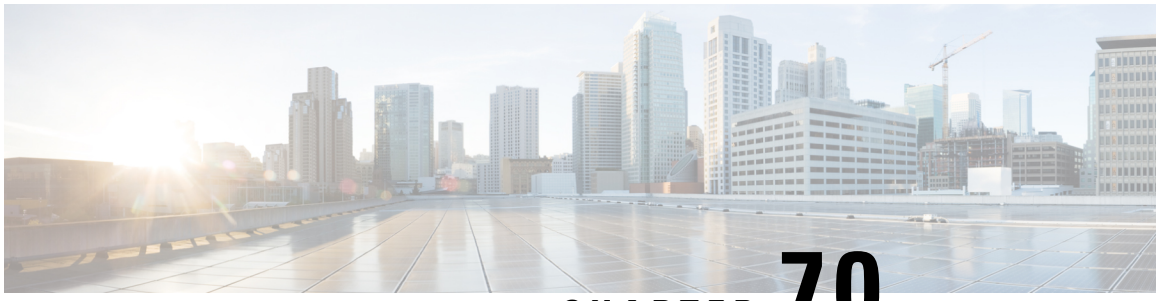
Client Load Based EDCA    : Enabled
```

To view the Adaptive EDCA parameters running on the driver, use the following command:

```
Device# show controllers dot11Radio 0/1

EDCA Config:
====================
L:Local C:Cell A:Adaptive EDCA params
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 4 6 3 0 0
AC_BK L 4 10 7 0 0
AC_VI L 3 4 1 94 0
AC_VO L 2 3 1 47 0
AC_BE C 4 10 3 0 0
AC_BK C 4 10 7 0 0
AC_VI C 3 4 2 94 0
AC_VO C 2 3 2 47 0
AC_BE A 4 10 7 0 0
AC_BK A 4 10 3 0 0
AC_VI A 3 4 2 94 0
AC_VO A 2 3 2 47 0
```



CHAPTER 69

802.11 parameters and Band Selection

- Information About Configuring Band Selection, 802.11 Bands, and Parameters, on page 779
- Restrictions for Band Selection, 802.11 Bands, and Parameters, on page 781
- How to Configure 802.11 Bands and Parameters, on page 781
- Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters, on page 791
- Configuration Examples for Band Selection, 802.11 Bands, and Parameters, on page 798

Information About Configuring Band Selection, 802.11 Bands, and Parameters

Band Select

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the device.

Band select works by regulating probe responses to clients and it can be enabled on a per-WLAN basis. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels. In an access point, the band select table can be viewed by running the **show dot11 band-select** command. It can also be viewed by running the **show cont d0/d1 | begin Lru** command.

Note You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

Band Select Algorithm

The band select algorithm affects clients that use 2.4-GHz band. Initially, when a client sends a probe request to an access point, the corresponding client probe's Active and Count values (as seen from the band select table) become 1. The algorithm functions based on the following scenarios:

- Scenario1: Client RSSI (as seen from the **show cont d0/d1** | **begin RSSI**command output) is greater than both Mid RSSI and Acceptable Client RSSI.

- Dual-band clients: No 2.4-GHz probe responses are seen at any time; 5-GHz probe responses are seen for all 5-GHz probe requests.
- Single-band (2.4-GHz) clients: 2.4-GHz probe responses are seen only after the probe suppression cycle.
- After the client's probe count reaches the configured probe cycle count, the algorithm waits for the Age Out Suppression time and then marks the client probe's Active value as 0. Then, the algorithm is restarted.

- Scenario2: Client RSSI (as seen from **show cont d0/d1** | **begin RSSI**) lies between Mid-RSSI and Acceptable Client RSSI.
  - All 2.4-GHz and 5-GHz probe requests are responded to without any restrictions.
  - This scenario is similar to the band select disabled.

Note The client RSSI value (as seen in the **sh cont d0** | **begin RSSI** command output) is the average of the client packets received, and the Mid RSSI feature is the instantaneous RSSI value of the probe packets. As a result, the client RSSI is seen as weaker than the configured Mid RSSI value (7-dB delta). The 802.11b probes from the client are suppressed to push the client to associate with the 802.11a band.

802.11 Bands

You can configure the 802.11b/g/n (2.4 GHz) and 802.11a/n (5 GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n are enabled.

This section contains the following subsections:

802.11n Parameters

This section provides instructions for managing 802.11n access points on your network. The 802.11n devices support the 2.4 and 5-GHz bands and offer high throughput data rates.

The 802.11n high throughput rates are available on all the 802.11n access points for the WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

Note To disable MCS rates for 802.11n, 802.11ac and 802.11ax, ensure that at least one MCS rate is enabled. To disable 802.11n on the controller to force APs to use only legacy 802.11a/b/g rates, first disable 802.11ax and 802.11ac on the controller for a particular band. Irrespective of the APs mapped to a Custom-RF-Profile, disabling 802.11n globally on the controller applies to all the APs.

802.11h Parameters

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

Restrictions for Band Selection, 802.11 Bands, and Parameters

- Band selection-enabled WLANs do not support time-sensitive applications such as voice and video because of roaming delays.
- Band selection is supported only on Cisco Wave 2 and 802.11ax APs.

  For more information about support on specific APs, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.
- Band selection operates only on APs that are connected to a controller. A FlexConnect AP without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same AP, and it only runs on an AP when both the 2.4-GHz and 5-GHz radios are up and running.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

How to Configure 802.11 Bands and Parameters

Configuring Band Selection (GUI)

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Wireless Advanced** > **Band Select**.

Step 2 In the **Cycle Count** field, enter a value between 1 and 10. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 3 In the **Cycle Threshold (milliseconds)** field, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 4 In the **Age Out Suppression (seconds)** field, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g/n clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 5 In the **Age Out Dual Band (seconds)** field, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 50 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 In the Client RSSI (dbm) field, enter a value between -90 to -20. This is the average of the client packets received.

Step 7 In the Client Mid RSSI (dbm) field, enter a value between -90 to -20. This the instantaneous RSSI value of the probe packets.

Step 8 On the **AP Join Profile** page, click the AP Join Profile name.

Step 9 Click **Apply**.

Configuring Band Selection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless client band-select cycle-count** *cycle_count* **Example:** `Device(config)# wireless client band-select cycle-count 3`	Sets the probe cycle count for band select. Valid range is between 1 and 10.
Step 3	**wireless client band-select cycle-threshold** *milliseconds* **Example:** `Device(config)# wireless client band-select cycle-threshold 5000`	Sets the time threshold for a new scanning cycle period. Valid range is between 1 and 1000.
Step 4	**wireless client band-select expire suppression** *seconds* **Example:** `Device(config)# wireless client band-select expire suppression 100`	Sets the suppression expire to the band select. Valid range is between 10 and 200.
Step 5	**wireless client band-select expire dual-band** *seconds* **Example:** `Device(config)# wireless client band-select expire dual-band 100`	Sets the dual band expire. Valid range is between 10 and 300.
Step 6	**wireless client band-select client-rssi** *client_rssi* **Example:** `Device(config)# wireless client band-select client-rssi 40`	Sets the client RSSI threshold. Valid range is between 20 and 90.
Step 7	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select** **Example:**	Configures band selection on specific WLANs. Valid range is between 1 and 512. You can enter up to 32 alphanumeric characters for *SSID_network_name* parameter.

	Command or Action	Purpose
	`Device(config)# wlan wlan1 25 ssid12` `Device(config-wlan)# band-select`	

Configuring the 802.11 Bands (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **Network**.

Step 2 Click either **5 GHz Band** or **2.4 GHz Band**.

Step 3 Uncheck the **Network Status** check box to disable the network in order to be able to configure the network parameters.

Step 4 In the **Beacon Interval** field, enter the rate at which the SSID is broadcast by the APs, from 100 to 600 milliseconds. The default is 100 milliseconds.

Step 5 For 802.11b/g/n (2.4-GHz) radios, to enable short preamble on the radio, check the **Short Preamble** check box. A short preamble improves throughput performance.

Step 6 In the **Fragmentation Threshold (in bytes)** field, enter a value between 256 to 2346 bytes. Packets larger than the size you specify here will be fragmented.

Step 7 Check the **DTPC Support** check box to advertise the transmit power level of the radio in the beacons and the probe responses. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there. You cannot configure a power constraint value on your 802.11a/n/ac (5-GHz) radio network if the **DTPC Support** check box is checked.

Step 8 Click **Apply**.

Step 9 In the **CCX Location Measurement** section, check the **Mode** check box to globally enable CCX radio management for the network. This parameter causes the APs connected to this device to issue broadcast radio measurement requests to clients running CCX v2 or later releases.

Step 10 In the **Interval** field, enter a value to specify how often the APs must issue broadcast radio measurement requests.

Step 11 Click **Apply**.

Step 12 In the **Data Rates** section, choose a value to specify the rates at which data can be transmitted between the access point and the client:

- Mandatory: Clients must support this data rate in order to associate to an access point on the controller embedded wireless controller.
- Supported: Any associated clients that support this data rate may communicate with the access point using that rate.
- Disabled: The clients specify the data rates used for communication.

Step 13 Click **Apply**.

Step 14 Save the configuration.

Configuring the 802.11 Bands (CLI)

Follow the procedure given below to configure 802.11 bands and parameters:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the 802.11a band. **Note** You must disable the 802.11a band before configuring the 802.11a network parameters.
Step 3	**ap dot11 24ghz shutdown** **Example:** `Device(config)# ap dot11 24ghz shutdown`	Disables the 802.11b band. **Note** You must disable the 802.11b band before configuring the 802.11b network parameters.
Step 4	**ap dot11 6ghz shutdown** **Example:** `Device(config)# ap dot11 6ghz shutdown`	Disables the 802.11 6-GHz band. **Note** You must disable the 802.11 6-GHz band before configuring the 802.11 6-GHz network parameters.
Step 5	**ap dot11** {**5ghz** | **24ghz** | **6ghz**} **beaconperiod** *time_unit* **Example:** `Device(config)# ap dot11 5ghz beaconperiod 500`	Specifies the rate at which the SSID is broadcast by the corresponding access point. The beacon interval is measured in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.
Step 6	**ap dot11** {**5ghz** | **24ghz** | **6ghz**} **fragmentation** *threshold* **Example:** `Device(config)# ap dot11 5ghz fragmentation 300`	Specifies the size at which packets are fragmented. The threshold is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 7	**[no] ap dot11** {**5ghz** | **24ghz** | **6ghz**} **dtpc**
	Example:
	`Device(config)# ap dot11 5ghz dtpc`
	`Device(config)# no ap dot11 24ghz dtpc`
		Enables access points to advertise their channels and transmit the power levels in beacons and probe responses.
		The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel-level and power-level

	Command or Action	Purpose
		information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan can rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there. The **no** form of the command disables the DTPC setting.
Step 8	**wireless client association limit** *number* **interval** *milliseconds* **Example:** `Device(config)# wireless client association limit 50 interval 1000`	Specifies the maximum allowed clients that can be configured. You can configure the maximum number of association requests on a single access point slot at a given interval. The range of association limit that you can configure is from 1 to 100. The association request limit interval is measured between 100 to 10000 milliseconds.
Step 9	**ap dot11 {5ghz | 24ghz} rate** *rate* {**disable** | **mandatory** | **supported**} **Example:** `Device(config)# ap dot11 5ghz rate 36 mandatory`	Specifies the rate at which data can be transmitted between the controller embedded wireless controller and the client. • **disable**: Defines that the clients specify the data rates used for communication. • **mandatory**: Defines that the clients support this data rate in order to associate to an access point on the controller embedded wireless controller. • **supported**: Any associated clients that support this data rate can communicate with the access point using that rate. However, the clients are not required to use this rate in order to associate. • *rate*: Specifies the rate at which data is transmitted. For the 802.11a and 802.11b bands, the data is transmitted at the rate of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.
Step 10	**no ap dot11 5ghz shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Enables the 802.11a band. **Note** The default value is enabled.
Step 11	**no ap dot11 24ghz shutdown**	Enables the 802.11b band.

	Command or Action	Purpose
	Example: `Device(config)# no ap dot11 24ghz shutdown`	**Note** The default value is enabled.
Step 12	**no ap dot11 6ghz shutdown** **Example:** `Device(config)# no ap dot11 6ghz shutdown`	Enables the 802.11 6-GHz band. **Note** The default value is enabled.
Step 13	**ap dot11 24ghz dot11g** **Example:** `Device(config)# ap dot11 24ghz dot11g`	Enables or disables 802.11g network support. The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.
Step 14	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring a Band-Select RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Advanced**.

Step 2 In the **Band Select** tab, enter a value between 1 and 10 in the **Cycle Count** field. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 3 In the **Cycle Threshold** field, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 4 In the **Age Out Suppression** field, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g/n clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 5 In the **Age Out Dual Band** field, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 50 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 In the **Client RSSI** field, enter a value between -90 dBm and -20 dBm. This is the minimum RSSI for a client to respond to a probe.

Step 7 In the **Client Mid RSSI** field, enter a value between –20 dBm and –90 dBm. This parameter sets the mid-RSSI, whose value can be used for toggling 2.4 GHz probe suppression based on the RSSI value.

Step 8 Click **Apply**.

Configuring a Band-Select RF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile test1`	Configures the RF profile name and enters RF profile configuration mode.
Step 3	**band-select client** {**mid-rssi** | **rssi** }*dbm* **Example:** `Device(config-rf-profile)# band-select client rssi -90`	Sets the band-select client threshold.
Step 4	**band-select cycle** {**count** | **threshold**}*count* **Example:** `Device(config-rf-profile)# band-select cycle count 10`	Sets the band-select cycle parameters.
Step 5	**band-select expire** {**dual-band** | **suppression** }*time* **Example:** `Device(config-rf-profile)# band-select expire dual-band 100`	Configures the RF profile's band-select expiry time.
Step 6	**band-select probe-response** **Example:** `Device(config-rf-profile)# band-select probe-response`	Enables the RF profile's band-select probe response.

Configuring 802.11n Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 Click **Add** to view the **Add RF Profile** window.

Step 3 In the **802.11** tab, proceed as follows:

a) Choose the required operational rates.

b) Select the required **802.11n MCS Rates** by checking the corresponding check boxes.

Step 4 Click **Save & Apply to Device**.

Configuring 802.11n Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz | 24ghz} dot11n** **Example:** `Device(config)# ap dot11 5ghz dot11n`	Enables 802.11n support on the network. The **no** form of this command disables the 802.11n support on the network.
Step 3	**ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu* **Example:** `Device(config)# ap dot11 5ghz dot11n mcs tx 20`	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. *rtu*-The valid range is between 0 and 23. The **no** form of this command disables the MCS rates that are configured.

Step 4	**wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require**
	Example:
	`Device(config)# wlan wlan1 25 ssid12`
	`Device(config-wlan)# wmm require`
		Enables WMM on the WLAN and uses the 802.11n data rates that you configured.
		The **require** keyword requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 5	**ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the network.
Step 6	**{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}** **Example:** `Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all`	Specifies the aggregation method used for 802.11n packets. Aggregation is the process of grouping packet data frames together, rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). Both A-MPDU and A-MSDU are performed in the software. You can specify the aggregation method for various types of traffic from the access point to the clients.

	Command or Action	Purpose
		The list defines the priority levels (0-7) assigned per traffic type. • 0—Best effort • 1—Background • 2—Spare • 3—Excellent effort • 4—Controlled load • 5—Video, less than 100-ms latency and jitter • 6—Voice, less than 100-ms latency and jitter • 7—Network control You can configure each priority level independently, or you can use the all the parameters to configure all the priority levels at once. You can configure priority levels so that the traffic uses either A-MPDU transmission or A-MSDU transmission. • When you use the **ap** command along with the other options, the traffic associated with that priority level uses A-MPDU transmission. • When you use the **no ap** command along with the other options, the traffic associated with that priority level uses A-MSDU transmission. Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4, and 5, and the rest are disabled. By default, A-MPDU is enabled for all priorities except 6 and 7.
Step 7	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Re-enables the network.
Step 8	**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}** **Example:**	Configures the guard interval for the network.

	Command or Action	Purpose
	`Device(config)# ap dot11 5ghz dot11n guard-interval long`	
Step 9	**ap dot11 {5ghz | 24ghz} dot11n rifs rx** **Example:** `Device(config)# ap dot11 5ghz dot11n rifs rx`	Configures the Reduced Interframe Space (RIFS) for the network.
Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11h Parameters (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap dot11 5ghz shutdown** **Example:** `Device(config)# ap dot11 5ghz shutdown`	Disables the 802.11 network.
Step 2	**ap dot11 6ghz shutdown** **Example:** `Device(config)# ap dot11 6ghz shutdown`	Disables the 802.11 6-GHz network.
Step 3	**{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode* **Example:** `Device(config)# ap dot11 5ghz channelswitch mode 0`	Enables or disables the access point to announce when it is switching to a new channel. *switch_mode*--Enter 0 or 1 to specify whether transmissions are restricted until the actual channel switch (**0**) or are not restricted (**1**). The default value is disabled.
Step 4	**[no] ap dot11 6ghz channelswitch quiet** **Example:** `Device(config)# ap dot11 5ghz channelswitch quiet`	Enables or disables the access point to announce when it is switching to a new channel in quiet mode.
Step 5	**ap dot11 5ghz power-constraint** *value* **Example:** `Device(config)# ap dot11 5ghz power-constraint 200`	Configures the 802.11h power constraint value in dB. The valid range is from 0 to 255. The default value is 3.
Step 6	**ap dot11 6ghz power-constraint** *value* **Example:**	Configures the 802.11 6-GHz power constraint value in dB. The valid range is from 0 to 30. The default value is 3.

	Command or Action	Purpose
	`Device(config)# ap dot11 5ghz power-constraint 200`	
Step 7	**no ap dot11 5ghz shutdown** **Example:** `Device(config)# no ap dot11 5ghz shutdown`	Re-enables the 802.11a network.
Step 8	**no ap dot11 6ghz shutdown** **Example:** `Device(config)# no ap dot11 6ghz shutdown`	Re-enables the 802.11 6-GHz network.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters

Verifying Configuration Settings Using Band Selection and 802.11 Bands Commands

The following commands can be used to verify band selection, 802.11 bands, and parameters on the .

Table 56: Monitoring Configuration Settings Using Band Selection and 802.11 Band Commands

Command	Purpose
show ap dot11 5ghz network	Displays 802.11a band network parameters, 802.11a operational rates, 802.11n MCS settings, and 802.11n status information.
show ap dot11 24ghz network	Displays 802.11b band network parameters, 802.11b/g operational rates, 802.11n MCS settings, and 802.11n status information.
show ap dot11 6ghz network	Displays 802.116-GHz band network parameters, 802.11b/g operational rates, 802.11n MCS settings, and 802.11n status information.
show wireless dot11h	Displays 802.11h configuration parameters.
show wireless band-select	Displays band-select configuration settings.

Example: Viewing the Configuration Settings for the 6-GHz Band

```
Device# show ap dot11 6ghz network
```

```
802.11 6Ghz Network                          : Enabled
802.11 6Ghz Status:
  A-MPDU Tx:
    Priority 0                               : Enabled
    Priority 1                               : Enabled
    Priority 2                               : Enabled
    Priority 3                               : Enabled
    Priority 4                               : Enabled
    Priority 5                               : Enabled
    Priority 6                               : Disabled
    Priority 7                               : Disabled
  A-MSDU Tx:
    Priority 0                               : Enable
    Priority 1                               : Enable
    Priority 2                               : Enable
    Priority 3                               : Enable
    Priority 4                               : Enable
    Priority 5                               : Enable
    Priority 6                               : Disable
    Priority 7                               : Disable
802.11ax                                     : Enabled
  DynamicFrag                                : Enabled
  MultiBssid                                 : Disabled
  Target Wakeup Time                         : Enabled
  Target Wakeup Time Broadcast               : Enabled
  BSS Color                                  : Disabled
  OBSS PD                                    : Disabled
  Non-SRG OBSS PD Maximum Threshold          : -62 dBm
  SRG OBSS PD                                : Disabled
  SRG OBSS PD Minimum Threshold              : -82 dBm
  SRG OBSS PD Maximum Threshold              : -62 dBm
802.11ax MCS Settings:
  MCS  7, Spatial Streams = 1                : Supported
  MCS  9, Spatial Streams = 1                : Disabled
  MCS 11, Spatial Streams = 1                : Supported
  MCS  7, Spatial Streams = 2                : Supported
  MCS  9, Spatial Streams = 2                : Disabled
  MCS 11, Spatial Streams = 2                : Supported
  MCS  7, Spatial Streams = 3                : Supported
  MCS  9, Spatial Streams = 3                : Disabled
  MCS 11, Spatial Streams = 3                : Supported
  MCS  7, Spatial Streams = 4                : Supported
  MCS  9, Spatial Streams = 4                : Disabled
  MCS 11, Spatial Streams = 4                : Supported
Beacon Interval                              : 95
CF Pollable mandatory                        : Disabled
CF Poll Request Mandatory                    : Disabled
CFP Period                                   : 4
CFP Maximum Duration                         : 60
Default Channel                              : 1
Default Tx Power Level                       : 1
DTPC Status                                  : Enabled
Fragmentation Threshold                      : 2335
RSSI Low Check                              : Disabled
RSSI Threshold                               : -127 dbm
TI Threshold                                 :
Legacy Tx Beamforming setting                : Disabled
Traffic Stream Metrics Status                : Disabled
Expedited BW Request Status                  : Disabled
EDCA profile type check                      : default-wmm
Client Load Based EDCA Config                : Enabled
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM)         : Disabled
```

```
  Voice Stream-Size                       : 84000
  Voice Max-Streams                       : 2
  Voice Max RF Bandwidth                  : 75
  Voice Reserved Roaming Bandwidth        : 6
  Voice Load-Based CAC mode               : Enabled
  Voice tspec inactivity timeout          : Enabled
CAC SIP-Voice configuration
  SIP based CAC                           : Disabled
  SIP call bandwidth                      : 64
  SIP call bandwidth sample-size           : 20
Maximum Number of Clients per AP Radio    : 200
WiFi to Cellular RSSI Threshold           : -85 dbm
Client Network Preference                 : default
```

Example: Viewing the Configuration Settings for the 5-GHz Band

```
Device# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
```

```
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwidth sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

Example: Viewing the Configuration Settings for the 2.4-GHz Band

```
Device# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

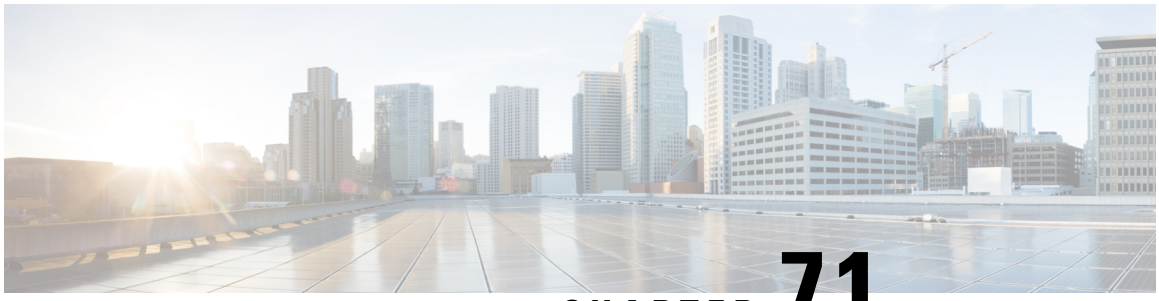
  802.11b/g Operational Rates
  802.11b 1M : Mandatory
  802.11b 2M : Mandatory
```

```
    802.11b 5.5M : Mandatory
    802.11g 6M : Supported
    802.11g 9M : Supported
    802.11b 11M : Mandatory
    802.11g 12M : Supported
    802.11g 18M : Supported
    802.11g 24M : Supported
    802.11g 36M : Supported
    802.11g 48M : Supported
    802.11g 54M : Supported
  802.11n MCS Settings:
    MCS 0 : Supported
    MCS 1 : Supported
    MCS 2 : Supported
    MCS 3 : Supported
    MCS 4 : Supported
    MCS 5 : Supported
    MCS 6 : Supported
    MCS 7 : Supported
    MCS 8 : Supported
    MCS 9 : Supported
    MCS 10 : Supported
    MCS 11 : Supported
    MCS 12 : Supported
    MCS 13 : Supported
    MCS 14 : Supported
    MCS 15 : Supported
    MCS 16 : Supported
    MCS 17 : Supported
    MCS 18 : Supported
    MCS 19 : Supported
    MCS 20 : Supported
    MCS 21 : Supported
    MCS 22 : Supported
    MCS 23 : Supported
  802.11n Status:
    A-MPDU Tx:
      Priority 0 : Enabled
      Priority 1 : Disabled
      Priority 2 : Disabled
      Priority 3 : Disabled
      Priority 4 : Enabled
      Priority 5 : Enabled
      Priority 6 : Disabled
      Priority 7 : Disabled
    A-MSDU Tx:
      Priority 0 : Enabled
      Priority 1 : Enabled
      Priority 2 : Enabled
      Priority 3 : Enabled
      Priority 4 : Enabled
      Priority 5 : Enabled
    Priority 6 : Disabled
      Priority 7 : Disabled
    Guard Interval : Any
    Rifs Rx : Enabled
  Beacon Interval : 100
  CF Pollable Mandatory : Disabled
  CF Poll Request Mandatory : Disabled
  CFP Period : 4
  CFP Maximum Duration : 60
  Default Channel : 11
  Default Tx Power Level : 1
  DTPC Status : true
```

```
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwidth sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

Example: Viewing the status of 802.11h Parameters

```
Device# show wireless dot11
Power Constraint: 0
Channel Switch : Enabled
Channel Switch Mode : Quiet
Smart DFS : Enabled
```

Example: Verifying the Band-Selection Settings

The following example displays a band-select configuration:

```
Device# show wireless band-select

Band Select Probe Response   : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : -80
Client Mid RSSI (dBm)        : -80
```

The following example displays an AP RF profile details:

```
Device# show ap rf-profile name vid detail

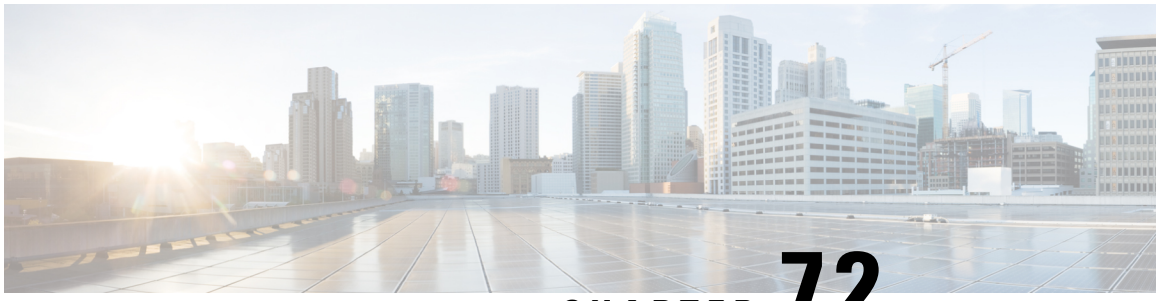
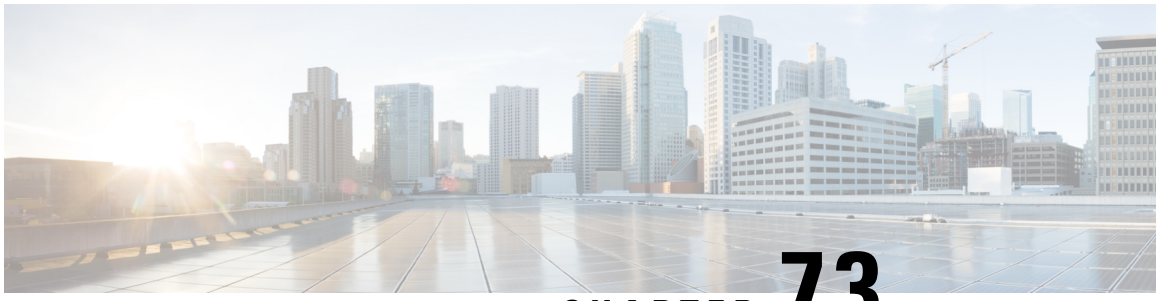
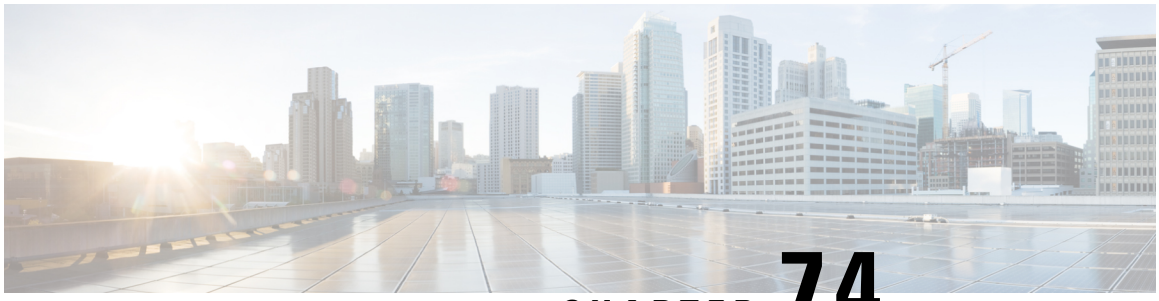
Description                     :
RF Profile Name                 : vid
```

```
Band                                : 2.4 GHz
802.11n client only                 : Disabled
Transmit Power Threshold v1         : -70 dBm
Min Transmit Power                  : -10 dBm
Max Transmit Power                  : 30 dBm
Operational Rates
  802.11b 1M Rate                   : Mandatory
  802.11b 2M Rate                   : Mandatory
  802.11b 5.5M Rate                 : Mandatory
  802.11b 11M Rate                  : Mandatory
  802.11b 6M Rate                   : Supported
  802.11b 9M Rate                   : Supported
  802.11b 12M Rate                  : Supported
  802.11b 18M Rate                  : Supported
  802.11b 24M Rate                  : Supported
  802.11b 36M Rate                  : Supported
  802.11b 48M Rate                  : Supported
  802.11b 54M Rate                  : Supported
Max Clients                         : 200
Trap Threshold
  Clients                           : 12 clients
  Interference                      : 10%
  Noise                             : -80 dBm
  Utilization                       : 10%
Multicast Data Rate                 : auto
Rx SOP Threshold                    : auto
Band Select
  Probe Response                    :  Disabled
  Cycle Count                       :  2 cycles
  Cycle Threshold                   :  200 milliseconds
  Expire Suppression                :  20 seconds
  Expire Dual Band                  :  60 seconds
  Client RSSI                       :  -80 dBm
  Client Mid RSSI                   :  -80 dBm
High Speed Roam
  hsr mode                          :  Disabled
  hsr neighbor timeout              :  5
Load Balancing
  Window                            :  5 clients
  Denial                            :  3 count
Coverage Data
  Data                              : -62 dBm
  Voice                             : -80 dBm
  Minimum Client Level              : 12 clients
  Exception Level                   : 48%
DCA Channel List                    : 1,6,11
Unused Channel List                 : 2,3,4,5,7,8,9,10
DCA Foreign AP Contribution         : Enabled
802.11n MCS Rates
  MCS  0                            : Enabled
  MCS  1                            : Enabled
  MCS  2                            : Enabled
  MCS  3                            : Enabled
  MCS  4                            : Enabled
  MCS  5                            : Enabled
  MCS  6                            : Enabled
  MCS  7                            : Enabled
  MCS  8                            : Enabled
  MCS  9                            : Enabled
  MCS 10                            : Enabled
  MCS 11                            : Enabled
  MCS 12                            : Enabled
  MCS 13                            : Enabled
  MCS 14                            : Enabled
```

```
  MCS 15                          : Enabled
  MCS 16                          : Enabled
  MCS 17                          : Enabled
  MCS 18                          : Enabled
  MCS 19                          : Enabled
  MCS 20                          : Enabled
  MCS 21                          : Enabled
  MCS 22                          : Enabled
  MCS 23                          : Enabled
  MCS 24                          : Enabled
  MCS 25                          : Enabled
  MCS 26                          : Enabled
  MCS 27                          : Enabled
  MCS 28                          : Enabled
  MCS 29                          : Enabled
  MCS 30                          : Enabled
  MCS 31                          : Enabled
State                             : Up
Client Network  Preference        : connectivity
```

Configuration Examples for Band Selection, 802.11 Bands, and Parameters

Examples: Band Selection Configuration

This example shows how to set the probe cycle count and time threshold for a new scanning cycle period for band select:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 3
Device(config)# wireless client band-select cycle-threshold 5000
Device(config)# end
```

This example shows how to set the suppression expiry time to the band select:

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 100
Device(config)# end
```

This example shows how to set the dual-band expiry time for the band select:

```
Device# configure terminal
Device(config)# wireless client band-select expire dual-band 100
Device(config)# end
```

This example shows how to set the client RSSI threshold for the band select:

```
Device# configure terminal
Device(config)# wireless client band-select client-rssi 40
Device(config)# end
```

This example shows how to configure band selection on specific WLANs:

```
Device# configure terminal
```

```
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# band-select
Device(config)# end
```

Examples: 802.11 Bands Configuration

This example shows how to configure 802.11 bands using beacon interval, fragmentation, and dynamic transmit power control:

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 24ghz shutdown
Device(config)# ap dot11 5ghz beaconperiod 500
Device(config)# ap dot11 5ghz fragmentation 300
Device(config)# ap dot11 5ghz dtpc
Device(config)# wireless client association limit 50 interval 1000
Device(config)# ap dot11 5ghz rate 36 mandatory
Device(config)# no ap dot11 5ghz shutdown
Device(config)# no ap dot11 24ghz shutdown
Device(config)# ap dot11 24ghz dot11g
Device(config)#end
```

Examples: 802.11n Configuration

This example shows how to configure 802.11n parameters for 5-GHz band using aggregation method:

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
Device(config)# no ap dot11 5ghz shutdown
Device(config)#exit
```

This example shows how to configure the guard interval for 5-GHz band:

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# no ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n guard-interval long
Device(config)#end
```

This example shows how to configure the RIFS for 5-GHz band:

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
```

```
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n rifs rx
Device(config)#end
```

Examples: 802.11h Configuration

This example shows how to configure the access point to announce when it is switching to a new channel using restriction transmission:

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz channelswitch mode 0
Device(config)# no ap dot11 5ghz shutdown
Device(config)#end
```

This example shows how to configure the 802.11h power constraint for 5-GHz band:

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz power-constraint 200
Device(config)# no ap dot11 5ghz shutdown
Device(config)#end
```



CHAPTER 70

NBAR Protocol Discovery

- Introduction to NBAR Protocol Discovery, on page 801
- Configuring NBAR Protocol Discovery, on page 801
- Verifying Protocol Discovery Statistics, on page 802

Introduction to NBAR Protocol Discovery

The NBAR Protocol Discovery feature provides an easy way of discovering the application protocols passing through an interface. Network Based Application Recognition (NBAR) determines which protocols and applications are currently running on the network. With Protocol Discovery, you can discover any protocol traffic that is supported by NBAR and obtain statistics that are associated with that protocol.

NBAR provides several classification features that identify applications and protocols from Layer 4 through Layer 7. NBAR is also used in Cisco Application Visibility and Control (AVC). With AVC, NBAR provides better application performance through better QoS and policing, and provides finer visibility about the network that is being used.

Configuring NBAR Protocol Discovery

Follow the procedure given below to enable protocol discovery:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy nbar-proto-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures the wireless policy profile for central switching. **Note** NBAR Protocol Discovery is supported in local mode (central switching) and in FlexConnect (central switching) mode.
Step 4	**ip nbar protocol-discovery** **Example:** `Device(config-wireless-policy)# ip nbar protocol-discovery`	Enables application recognition on the wireless policy profile by activating the NBAR2 engine.

Verifying Protocol Discovery Statistics

To view protocol discovery statistics, use the following command:

```
Device# show ip nbar protocol-discovery wlan wlan-profile-name

wlan_profile_name (iif_id 0xF0400002)

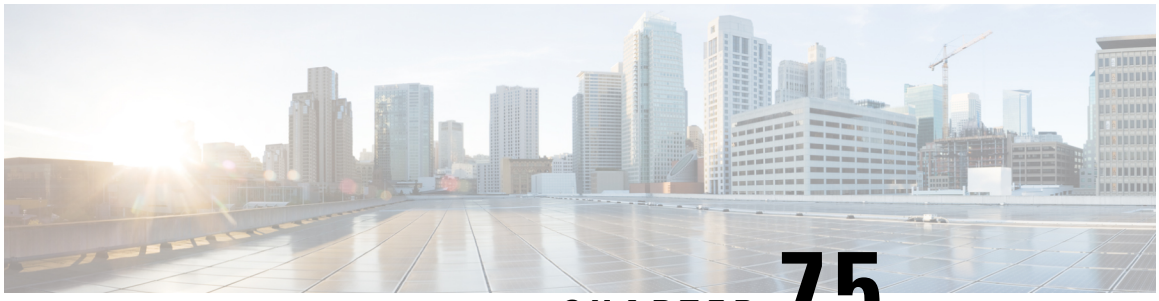
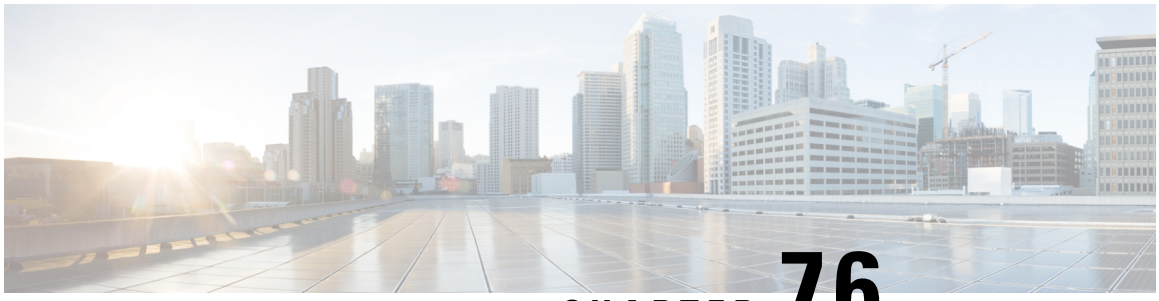
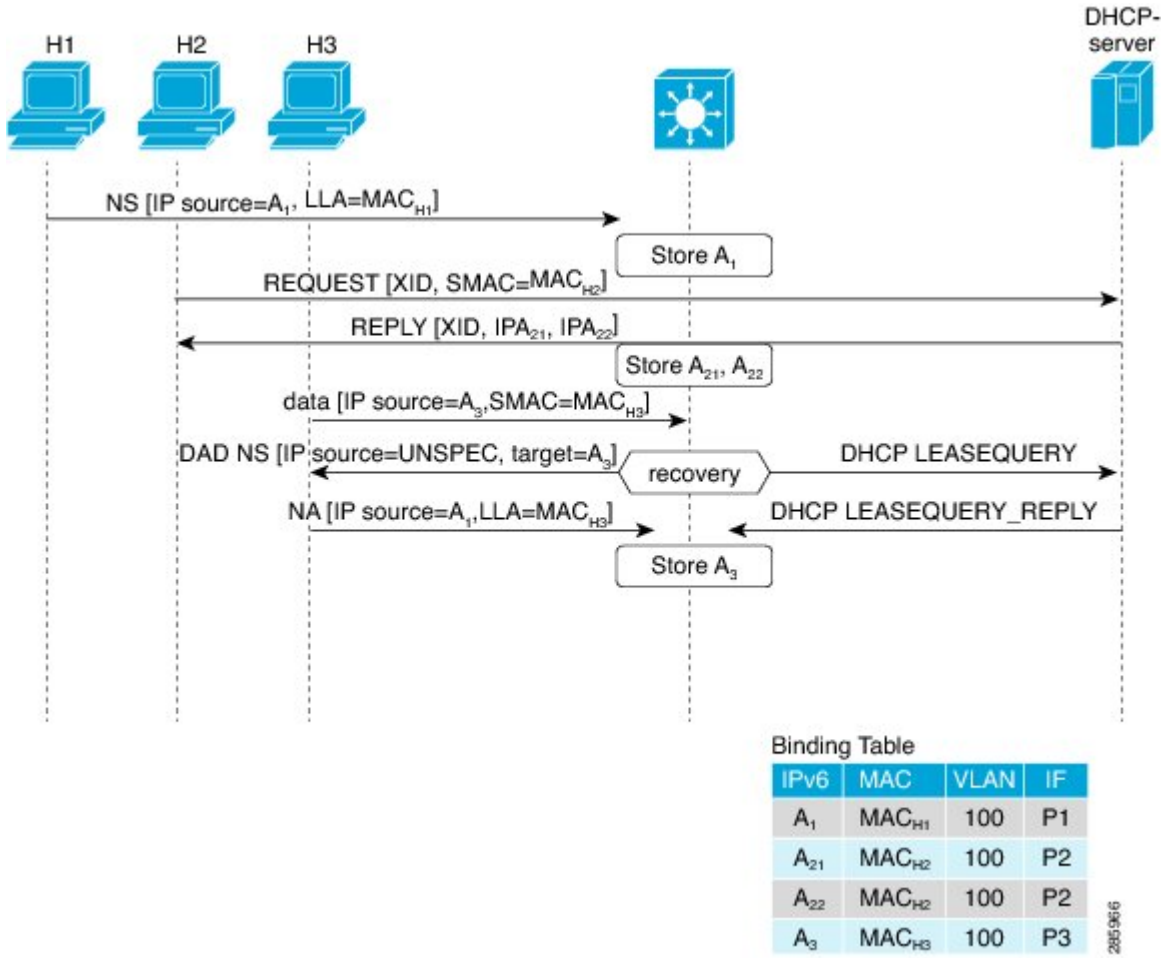
Last clearing of "show ip nbar protocol-discovery" counters 00:07:12


                         Input                    Output
                         -----                    ------
   Protocol              Packet Count             Packet Count
                         Byte Count               Byte Count
                         5min Bit Rate (bps)      5min Bit Rate (bps)
                         5min Max Bit Rate (bps)  5min Max Bit Rate (bps)
   ----------------------- ------------------------ ------------------------
   unknown               22                       0
                         4173                     0
                         0                        0
                         2000                     0
   dhcp                  3                        2
                         1166                     724
                         0                        0
                         0                        0
   ping                  2                        2
                         204                      236
                         0                        0
                         0                        0
   Total                 27                       4
                         5543                     960
                         0                        0
                         2000                     0
```

To clear protocol discovery statistics, use the following command:

```
Device# clear ip nbar protocol-discovery wlan wlan-profile-name
```



CHAPTER 71

Conditional Debug, Radioactive Tracing, and Packet Tracing

- Introduction to Conditional Debugging, on page 803
- Introduction to Radioactive Tracing, on page 804
- Conditional Debugging and Radioactive Tracing, on page 804
- Location of Tracefiles, on page 805
- Configuring Conditional Debugging (GUI), on page 805
- Configuring Conditional Debugging, on page 806
- Radioactive Tracing for L2 Multicast, on page 807
- Recommended Workflow for Trace files, on page 807
- Copying Tracefiles Off the Box, on page 808
- Configuration Examples for Conditional Debugging, on page 808
- Verifying Conditional Debugging, on page 809
- Example: Verifying Radioactive Tracing Log for SISF, on page 809
- Information About Packet Tracing, on page 810
- Configuring Conditional Debugging Packet Tracing, on page 811
- Configuring Conditional Debugging Packet Tracing per AP, on page 812
- Configuring Conditional Debugging Packet Tracing per Client (GUI), on page 813
- Configuring Conditional Debugging Packet Tracing per Client, on page 813
- Verifying Conditional Debugging Packet Tracing Configuration, on page 813

Introduction to Conditional Debugging

The Conditional Debugging feature allows you to selectively enable debugging and logging for specific features based on the set of conditions you define. This feature is useful in systems where a large number of features are supported.

The Conditional debug allows granular debugging in a network that is operating at a large scale with a large number of features. It allows you to observe detailed debugs for granular instances within the system. This is very useful when we need to debug only a particular session among thousands of sessions. It is also possible to specify multiple conditions.

A condition refers to a feature or identity, where identity could be an interface, IP Address, or a MAC address and so on.

This is in contrast to the general debug command, that produces its output without discriminating on the feature objects that are being processed. General debug command consumes a lot of system resources and impacts the system performance.

Introduction to Radioactive Tracing

Radioactive tracing (RA) provides the ability to stitch together a chain of execution for operations of interest across the system, at an increased verbosity level. This provides a way to conditionally print debug information (up to DEBUG Level or a specified level) across threads, processes and function calls.

Note

- The radioactive tracing supports First-Hop Security (FHS).

  For more information on First Hop Security features, see *System Management > Wireless Multicast > Information About Wireless Multicast > Information About IPv6 Snooping*.

- The radioactive tracing filter does not work, if the certificate is not valid.
- For effective debugging of issues on mesh features, ensure that you add both Ethernet and Radio MAC address as conditional MAC for RA tracing, while collecting logs.
- To enable debug for wireless IPs, use the **debug platform condition feature wireless ip** *ip-address* command.

Table 57: Components Supporting Radio Active Tracing

Components	Details
SISF or FHS	The first-hop security features, includes IPv6 Address Glean and IPv6 Device Tracking. For more information, see *Information About IPv6 Snooping*.
LISP	Locator or ID Separation Protocol.

Conditional Debugging and Radioactive Tracing

Radioactive Tracing when coupled with Conditional Debugging, enable us to have a single debug CLI to debug all execution contexts related to the condition. This can be done without being aware of the various control flow processes of the feature within the box and without having to issue debugs at these processes individually.

Note Use the **clear platform condition all** command to remove the debug conditions applied to the platform.

Location of Tracefiles

By default the tracefile logs will be generated for each process and saved into either the **/tmp/rp/trace** or **/tmp/fp/trace** directory. In this temp directory, the trace logs are written to files, which are of 1 MB size each. You can verify these logs (per-process) using the **show platform software trace message** *process_name* **chassis active R0** command. The directory can hold up to a maximum of 25 such files for a given process. When a tracefile in the **/tmp** directory reaches its 1MB limit or whatever size was configured for it during the boot time, it is rotated out to an archive location in the **/crashinfo** partition under **tracelogs** directory.

The **/tmp** directory holds only a single tracefile for a given process. Once the file reaches its file size limit it is rotated out to **/crashinfo/tracelogs**. In the archive directory, up to 25 files are accumulated, after which the oldest one is replaced by the newly rotated file from **/tmp**. File size is process dependent and some processes uses larger file sizes (upto 10MB). Similarly, the number of files in the **tracelogs** directory is also decided by the process. For example, WNCD process uses a limit of 400 files per instance, depending on the platform.

The tracefiles in the crashinfo directory are located in the following formats:

1. Process-name_Process-ID_running-counter.timestamp.gz

   Example: IOSRP_R0-0.bin_0.14239.20151101234827.gz

2. Process-name_pmanlog_Process-ID_running-counter.timestamp.bin.gz

   Example: wncmgrd_R0-0.27958_1.20180902081532.bin.gz

Configuring Conditional Debugging (GUI)

Procedure

Step 1	Choose **Troubleshooting** > **Radioactive Trace**.
Step 2	Click **Add**.
Step 3	Enter the **MAC/IP Address**. The MAC address can be either in *xx:xx:xx:xx:xx:xx*, *xx-xx-xx-xx-xx-xx*, or *xxxx.xxxx.xxxx* format.
Step 4	Click **Apply to Device**.
Step 5	Click **Start** to start or **Stop** to stop the conditional debug.
Step 6	Click **Generate** to create a radioactive trace log.
Step 7	Click the radio button to set the time interval.
Step 8	Click the **Download Logs** icon that is displayed next to the trace file name, to download the logs to your local folder.
Step 9	Click the **View Logs** icon that is displayed next to the trace file name, to view the log files on the GUI page. Click **Load More** to view more lines of the log file.
Step 10	Click **Apply to Device**.

Configuring Conditional Debugging

Follow the procedure given below to configure conditional debugging:

Procedure

	Command or Action	Purpose
Step 1	**debug platform condition feature wireless mac** {*mac-address*} **Example:** `Device# debug platform condition feature wireless mac b838.61a1.5433`	Configures conditional debugging for a feature using the specified MAC address. **Note** This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.
Step 2	**debug platform condition start** **Example:** `Device# debug platform condition start`	Starts conditional debugging (this will start radioactive tracing if there is a match on one of the conditions above). **Note** This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.

Step 3	**show platform condition** OR **show debug**
	Example:
	`Device# show platform condition`
	`Device# show debug`
		Displays the current conditions set.

Step 4	**debug platform condition stop** **Example:** `Device# debug platform condition stop`	Stops conditional debugging (this will stop radioactive tracing). **Note** This is supported with AP or client MAC/IP and also on CMX IP address and mobility peer IP.
Step 5	**show logging profile wireless** [**counter** | **[last]**{*x days/hours*} | **filter mac**{<*mac address*>} **[to-file]**{<*destination*>} **Example:** `Device# show logging profile wireless start last 20 minutes to-file bootflash:logs.txt`	Displays the logs from the latest wireless profile. **Note** You can use either the *show logging profile wireless* command or *show logging process* command to collect the logs.
Step 6	**show logging process** <*process name*> **Example:** `Device# show logging process wncd to-file flash:wncd.txt`	Displays the logs collection specific to the process.

	Command or Action	Purpose
Step 7	**clear platform condition all** **Example:** `Device# clear platform condition all`	Clears all conditions.

What to do next

Note The command **request platform software trace filter-binary wireless** {*mac-address*} generates 3 flash files:

- *collated_log_<.date..>*
- *mac_log <..date..>*
- *mac_database .. file*

Of these, *mac_log <..date..>* is the most important file, as it gives the messages for the MAC address we are debugging. The command **show platform software trace filter-binary** also generates the same flash files, and also prints the mac_log on the screen.

Radioactive Tracing for L2 Multicast

To identify a specific multicast receiver, specify the MAC address of the joiner or the receiver client, Group Multicast IP address and Snooping VLAN. Additionally, enable the trace level for the debug. The debug level will provide detailed traces and better visibility into the system.

debug platform condition feature multicast controlplane mac *client-mac-addr* **ip** *group-ip-addr* **vlan** *id* **level** *debug level*

Recommended Workflow for Trace files

The Recommended Workflow for Trace files is listed below:

1. To request the tracelogs for a specific time period.

   EXAMPLE 1 day.

   Use the command:

   Device#**show logging process wncd to-file flash:wncd.txt**

2. The system generates a text file of the tracelogs in the location /flash:
3. Copy the file off the switchdevice. By copying the file, the tracelogs can be used to work offline. For more details on copying files, see section below.
4. Delete the tracelog file (.txt) file from /flash: location. This will ensure enough space on the switchdevice for other operations.

Copying Tracefiles Off the Box

An example of the tracefile is shown below:

```
Device# dir crashinfo:/tracelogs
Directory of crashinfo:/tracelogs/

50664 -rwx 760 Sep 22 2015 11:12:21 +00:00 plogd_F0-0.bin_0.gz
50603 -rwx 991 Sep 22 2015 11:12:08 +00:00 fed_pmanlog_F0-0.bin_0.9558.20150922111208.gz
50610 -rw- 11 Nov 2 2015 00:15:59 +00:00 timestamp
50611 -rwx 1443 Sep 22 2015 11:11:31 +00:00
auto_upgrade_client_sh_pmanlog_R0-.bin_0.3817.20150922111130.gz
50669 -rwx 589 Sep 30 2015 03:59:04 +00:00 cfgwr-8021_R0-0.bin_0.gz
50612 -rwx 1136 Sep 22 2015 11:11:46 +00:00 reflector_803_R0-0.bin_0.1312.20150922111116.gz
50794 -rwx 4239 Nov 2 2015 00:04:32 +00:00 IOSRP_R0-0.bin_0.14239.20151101234827.gz
50615 -rwx 131072 Nov 2 2015 00:19:59 +00:00 linux_iosd_image_pmanlog_R0-0.bin_0
```

The trace files can be copied using one of the various options shown below:

```
Device# copy crashinfo:/tracelogs ?
  crashinfo: Copy to crashinfo: file system
  flash: Copy to flash: file system
  ftp: Copy to ftp: file system
  http: Copy to http: file system
  https: Copy to https: file system
  null: Copy to null: file system
  nvram: Copy to nvram: file system
  rcp: Copy to rcp: file system
  running-config Update (merge with) current system configuration
  scp: Copy to scp: file system
  startup-config Copy to startup configuration
  syslog: Copy to syslog: file system
  system: Copy to system: file system
  tftp: Copy to tftp: file system
  tmpsys: Copy to tmpsys: file system
```

The general syntax for copying onto a TFTP server is as follows:

```
Device# copy source: tftp:
Device# copy crashinfo:/tracelogs/IOSRP_R0-0.bin_0.14239.20151101234827.gz tftp:
Address or name of remote host []? 2.2.2.2
Destination filename [IOSRP_R0-0.bin_0.14239.20151101234827.gz]?
```

Note It is important to clear the generated report or archive files off the switch in order to have flash space available for tracelog and other purposes.

Configuration Examples for Conditional Debugging

The following is an output example of the *show platform condition* command.

```
Device# show platform condition
Conditional Debug Global State: Stop
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|----------------------|--------------------------------
Device#
```

The following is an output example of the *show debug* command.

```
Device# show debug
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Start
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|----------------------|--------------------------------
Packet Infra debugs:
Ip Address Port
------------------------------------------------------|----------
Device#
```

Verifying Conditional Debugging

The table shown below lists the various commands that can be used to verify conditional debugging:

Command	Purpose
show platform condition	Displays the current conditions set.
show debug	Displays the current debug conditions set.
show platform software trace filter-binary	Displays logs merged from the latest tracefile.
request platform software trace filter-binary	Displays historical logs of merged tracefiles on the system.

Example: Verifying Radioactive Tracing Log for SISF

The following is an output example of the *show platform software trace message ios chassis active R0 | inc sisf* command.

```
Device# show platform software trace message ios chassis active R0 | inc sisf

2017/10/26 13:46:22.104 {IOSRP_R0-0}{1}: [parser]: [5437]:  UUID: 0, ra: 0 (note):  CMD:
'show platform software trace message ios switch active R0 | inc sisf' 13:46:22 UTC Thu Oct
 26 2017
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
   FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Unlocking, count is now 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
   FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Unlocking, count is now 1
```

```
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Setting State to 2
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Start timer 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc  Timer value/granularity for 0 :299998/1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Updated Mac Timer : 299998
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Before Timer :  350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Timer 0, default value is 350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
   Allocating timer wheel for 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc No timer running
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Granularity for timer MAC_T1  is 1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7 (debug):
  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Current State :MAC-STALE, Req Timer : MAC_T1  Current Timer
 MAC_T1
```

Information About Packet Tracing

The Packet tracing feature cover details on how to perform data plane packet tracing for Cisco Catalyst 9800 Series Wireless Controller for Cloud software.

This feature identifies the following issues:

- Misconfiguration
- Capacity overload
- Software bugs while troubleshooting

This feature identifies what happens to a packet in your system. The conditional debugging packet tracing feature is used for accounting and capturing per-packet processing details for user-defined conditions.

You can trace packets on the controller using the following steps:

1. Enable conditional debugging on selected packets or traffic you want to trace on the controller.
2. Enable packet tracing (per-AP or per-Client).

Note You need to use per AP conditional debugging with MAC address as a filter when AP and controllers are in the same VLAN. If they are not in the same VLAN, the per AP packet tracing with MAC address does not capture packets as MAC address varies.

Limitation of Conditional Debugging Packet Tracing

MAC or IP filter only applies to the outer Ethernet or IP header, so if a packet is CAPWAP encapsulated, the MAC or IP does not apply to the inner 802.11 MAC or IP.

Configuring Conditional Debugging Packet Tracing

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**debug platform packet-trace packet** *packet-count* **circular fia-trace data-size** *data-size* **Example:** `Device# debug platform packet-trace packet 8192 circular fia-trace data-size 2048`	Configures packet tracing to capture the last set of packets. Here, *packet-count*—Valid range is from 16 to 8192. *data-size*—Valid range is from 2048 to 16384 bytes.
Step 3	**debug platform packet-trace copy packet both size** *packet-size* **Example:** `Device# debug platform packet-trace copy packet both size 2048`	Configures packet tracing for a copy of packet data. Here, *packet-size*—Valid range is from 16 to 2048 bytes.
Step 4	**debug platform condition interface** {*intf-name* | **cpp**} {**mac** | **ipv4** | **match**} {**both** | **ingress** | **egress**} **Example:** Enables conditional debugging for TenGigabitEthernet 0/0/0 and match packets whose source and destination MAC is 0001.0001.0001: `Device# debug platform condition interface TenGigabitEthernet 0/0/0 mac 0001.0001.0001 both`	Enables conditional debugging for an interface, MAC, or IP filter. An interface refers to any physical port, port channel, internal vlan, SVI, or wireless client.
Step 5	**debug platform condition start** **Example:** `Device# debug platform condition start`	Starts conditional debugging packet tracing.
Step 6	**debug platform condition stop** **Example:** `Device# debug platform condition stop`	Stops conditional debugging packet tracing.
Step 7	**show platform hardware chassis active qfp feature packet-trace packet all | redirect bootflash:packet_trace.txt**	Redirects all traced packets to bootflash.

	Command or Action	Purpose
	Example: `Device# show platform hardware chassis active qfp feature packet-trace packet all | redirect bootflash:packet_trace.txt`	Converts the packet_trace.txt to pcap and downloads the pcap files. You can do so using the following link: http://wwwin-dharton-dev.cisco.com/pactrac2pcap.html

Configuring Conditional Debugging Packet Tracing per AP

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.

Step 2	**debug platform condition interface** {*intf-name* | **cpp**} {**mac** [**mac-address** | **access-list** *acl-name*] | **ipv4** | **match**} {**both** | **ingress** | **egress**}
	Example:
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 mac 0001.0001.0001 both`
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 mac access-list mac-acl-name both`
		Enables conditional debugging with MAC filter.
		Herein, the CLI matches the packets whose source or destination MAC address is 0001.0001.0001.

Step 3	**debug platform condition interface TenGigabitEthernet** *intf-number* **match mac** {**H.H.H** | **any** | **host**} {**both** | **ingress** | **egress**} **Example:** `Device# debug platform condition interface TenGigabitEthernet 0/0/0 match mac 0001.0001.0001 both`	Enables conditional debugging with inline MAC ACL.

Step 4	**debug platform condition interface TenGigabitEthernet** *intf-number* **ipv4** {*A.B.C.D/nn* | **access-list** *acl-name* | **both** | **egress** | **ingress**} {**both** | **egress** | **ingress**}
	Example:
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 ipv4 192.168.1.2/32 both`
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 ipv4 access-list ip-acl-name both`
		Enables conditional debugging with IP filter.
		Here,
		intf-number—Is the GigabitEthernet interface number.Valid range is from 1 to 32.

	Command or Action	Purpose
	`Device# debug platform condition interface TenGigabitEthernet 0/0/0 match ipv4 192.168.1.2/32 both`	

Configuring Conditional Debugging Packet Tracing per Client (GUI)

Procedure

Step 1 Choose **Troubleshooting** > **Radioactive Trace**.

Step 2 Click **Add**.

Step 3 In the Add MAC/IP Address window, enter the **MAC/IP Address**.

Step 4 Click **Apply to Device**.

Configuring Conditional Debugging Packet Tracing per Client

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**debug platform condition interface** {*intf-name* | **cpp** *cpp-handle-index*} {**mac** | **ipv4** | **match** [**ipv4** | **ipv6** | **mac**]} {**both** | **ingress** | **egress**} **Example:** `Device# debug platform condition interface cpp 0xa0000001 match ipv4 protocol icmp host 192.168.1.100 host 192.168.1.1 both`	Enables conditional debugging for a wireless client interface. Here, *cpp-handle-index*—Valid range is from 1 to 4294967295.

Verifying Conditional Debugging Packet Tracing Configuration

To view the summary of the traced packet, use the following command:

```
Device# show platform packet-trace summary
```

To view a specific traced packet, use the following command:

```
Device# show platform packet-trace packet packet-number
```

To view the wireless client interface handle, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
mac-address client-mac details
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
mac-address 8825.93b0.b51f details
Client Details for client cpp_if_handle: 0x34
Name : WLCLIENT-IF-0x00a0000001
Mac Addr : 8825.93b0.b51f
pal_if_handle : 0xa0000001
Mobility State : LOCAL
Multicast Action : FORWARD
Auth State : RUN
```



CHAPTER 72

Aggressive Client Load Balancing

- Information About Aggressive Client Load Balancing, on page 815
- Enabling Aggressive Client Load Balancing (GUI), on page 816
- Configuring Aggressive Client Load Balancing (GUI), on page 816
- Configuring Aggressive Client Load Balancing (CLI), on page 817

Information About Aggressive Client Load Balancing

The Aggressive Client Load Balancing feature allows lightweight access points to load balance wireless clients across access points.

When a wireless client attempts to associate to a lightweight access point, the associated response packets are sent to a client with an 802.11 response packet including status code 17. This code 17 indicates that the corresponding AP is busy. The AP does not respond with the response 'success' if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is exceeded, and another less busy AP hears the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 and the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, the client receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempts to associate 11 times, it will be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients, such as time-sensitive voice clients.

Note A voice client does not authenticate when delay is configured to more than 300 ms. To avoid this, configure a central-authentication, local-switching WLAN with Cisco Centralized Key Management (CCKM), configure a pagent router between an AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN), and try associating the voice client.

Note For a FlexConnect AP, the association is locally handled. The load-balancing decisions are taken at the controller. A FlexConnect AP sends an initial response to the client before knowing the result of the calculations in the controller. Load-balancing does not take effect when the FlexConnect AP is in standalone mode.

A FlexConnect AP does not send (re)association response with status 17 for load balancing the way local-mode APs do; instead, it first sends (re)association with status 0 (success) and then deauth with reason 5.

Note This feature is not supported on the APs joined on default-site-tag.

This feature is not supported on the APs across different named site-tags.

This feature is supported only on the APs within a named-site-tag.

Enabling Aggressive Client Load Balancing (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > WLANs > Wireless Networks**.

Step 2 Select a **WLAN** to view the **Edit WLAN** window.

Step 3 Click **Advanced** tab.

Step 4 Select the **Load Balance** check box to enable the feature.

Step 5 Click **Update & Apply to Device**.

Configuring Aggressive Client Load Balancing (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Advanced**.

The **Load Balancing** window is displayed.

Step 2 In the **Aggressive Load Balancing Window (clients)** field, enter the number of clients for the aggressive load balancing client window.

Step 3 In the **Aggressive Load Balancing Denial Count** field, enter the load balancing denial count.

Step 4 Click **Apply**.

Configuring Aggressive Client Load Balancing (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name* **Example:** `Device(config)# wlan test-wlan`	Specifies the WLAN name.
Step 4	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 5	**load-balance** **Example:** `Device(config-wlan)# load-balance`	Configures a guest controller as mobility controller, in order to enable client load balance to a particular WLAN. Configure the WLAN security settings as the WLAN requirements.
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables WLAN.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 9	**ap dot11** {**24ghz** | **5ghz**} **load-balancing denial** *denial-count* **Example:** `Device(config)# ap dot11 5ghz load-balancing denial 10`	Configures the load balancing denial count.

	Command or Action	Purpose
Step 10	**ap dot11** {**24ghz** | **5ghz**} **load-balancing window** *number-of-clients* **Example:** `Device(config)# ap dot11 5ghz load-balancing window 10`	Configures the number of clients for the aggressive load balancing client window.
Step 11	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.
Step 12	**show running-config | section** *wlan-name* **Example:** `Device# show running-config | section test-wlan`	Displays a filtered section of the current configuration.



CHAPTER 73

Accounting Identity List

- Configuring Accounting Identity List (GUI), on page 819
- Configuring Accounting Identity List (CLI), on page 819
- Configuring Client Accounting (GUI), on page 820
- Configuring Client Accounting (CLI), on page 820

Configuring Accounting Identity List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**.

Step 2 In the **AAA Method List** tab, go to the **Accounting** section, and click **Add**.

Step 3 In the **Quick Setup: AAA Accounting** window that is displayed, enter a name for your method list.

Step 4 Choose the type of authentication as identity, in the **Type** drop-down list.

Step 5 Choose the server groups you want to use to authenticate access to your network, from the **Available Server Groups** list and click > icon to move them to the **Assigned Server Groups** list.

Step 6 Click **Save & Apply to Device**.

Configuring Accounting Identity List (CLI)

Accounting is the process of logging the user actions and keeping track of their network usage. Whenever a user successfully executes an action, the RADIUS accounting server logs the changed attributes, the user ID of the person who made the change, the remote host where the user is logged in, the date and time when the command was executed, the authorization level of the user, and a description of the action performed and the values provided.

Follow the procedure given below to configure accounting identity list.

Before you begin

Configure the RADIUS server and AAA group server.

Procedure

	Command or Action	Purpose
Step 1	**aaa accounting identity** *named-list* **start-stop group** *server-group-name* **Example:** `Device(config)# aaa accounting identity user1 start-stop group aaa-test`	Enables accounting to send a start-record accounting notice when a client is authorized and a stop-record at the end. **Note** You can also use the default list, instead of a named list.

Whenever there is a change in the client attribute, for example, change in IP address, client roaming, and so on, an accounting interim update is sent to the RADIUS server.

Configuring Client Accounting (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the **Policy Profile Name** and in the **Edit Policy Profile** window, go to the **Advanced** tab.

Step 3 From the **Accounting List** drop-down, select the appropriate accounting list for this policy profile. This will ensure that the policy profile undergoes that type of accounting you want to perform, before allowing it access to the network.

Step 4 Click **Save & Apply to Device**.

Configuring Client Accounting (CLI)

Follow the procedure given below to configure client accounting.

Before you begin

Ensure that RADIUS accounting is configured.

Procedure

	Command or Action	Purpose
Step 1	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 2	**shutdown** **Example:**	Disables the policy profile.

	Command or Action	Purpose
	`Device(config-wireless-policy)# shutdown`	
Step 3	**accounting-list** *list-name* **Example:** `Device(config-wireless-policy)# accounting-list user1`	Sets the accounting list.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.



CHAPTER 74

Support for Accounting Session ID

- Information About Accounting Session ID, on page 823
- Configuring an Accounting Session ID (CLI), on page 823
- Verifying an Account Session ID, on page 824

Information About Accounting Session ID

Accounting ID is a unique identifier for a wireless client session. This ID helps to identify the accounting data of a client in the AAA server. Accounting session ID is generated by the AAA module.

From Cisco IOS XE Bengaluru, Release 17.4.1 onwards, Accounting Session ID is supported in the AAA access request, while authenticating wireless client using IEEE 802.1x method. In the Cisco IOS XE Amsterdam, Release 17.3.x and earlier releases, the Accounting Session ID was sent only as part of the accounting request. From Cisco IOS XE Bengaluru, Release 17.4.1 onwards, the Accounting Session ID is sent as part of the access request too.

Configuring an Accounting Session ID (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius-server attribute wireless 44 include-in-access-req** **Example:** `Device(config)# radius-server attribute wireless 44 include-in-access-req`	Sends the RADIUS authentication attribute 44, in the access request packet.
Step 3	**aaa accounting identity** *accounting-list-name* **start-stop group** *server-group-name* **Example:**	Configures the accounting session identity of the AAA server.

	Command or Action	Purpose
	`Device(config)# aaa accounting identity` *`accounting-list-name`* `start-stop group` *`AAA_GROUP_1`*	
Step 4	**wireless profile policy** **Example:** `Device(config)# wireless profile policy` `default-policy-profile` *`accounting-list-name`* `start-stop group` *`AAA_GROUP_1`*	Configures the WLAN policy profile.
Step 5	**accounting-list** *accounting-list-name* **Example:** `Device(config-wireless-policy)# accounting-list` *`accounting-list-name`*	Configures the accounting list. **Note** The Accounting Session ID is added as part of the account request, only if **radius-server attribute wireless 44 include-in-access-req** is enabled along with the accounting configuration under the wireless policy.
Step 6	**description** *description-name* **Example:** `Device(config-wireless-policy)# description` *`accounting-description`*	Adds a description for the policy profile.
Step 7	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan` *`40`*	Configures the VLAN name or ID.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

Verifying an Account Session ID

To verify if an Account Session ID is populated, use the following command:

```
Device# show wireless pmk-cache
Number of PMK caches in total : 1
Type      Station            Entry Lifetime  VLAN Override         IP Override
Accounting-Session-Id   Audit-Session-Id              Username

-----------------------------------------------------------------------------------------------

RSN       6c19.c0e6.a444      1768            NA
0x00000006              052DA8C1000000104E634C77      cwa-user
```

To display the current Accounting Session ID, use the following command:

```
Device# show wireless client mac-address<H.H.H>detail
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90000005
  IIF ID              : 0x90000005
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 000000000000000B14E9130A
  Acct Session ID  : 0x0000000c
  Last Tried Aaa Server Details:
        Server IP : 9.10.8.247
  Auth Method Status List
        Method : Dot1x
                 SM State         : AUTHENTICATED
                 SM Bend State    : IDLE
  Local Policies:
        Service Template : wlan_svc_default-policy-profile (priority 254)
                 VLAN             : 1
  Server Policies:
                 Absolute-Timer   : 1800
  Resultant Policies:
                 VLAN Name        : default
                 VLAN             : 1
                 Absolute-Timer   : 1800
```



CHAPTER 75

Interim Accounting

- Information About Interim Accounting, on page 827
- Disabling Interim Accounting (CLI), on page 828
- Verifying Interim Accounting, on page 828

Information About Interim Accounting

RADIUS accounting sends accounting-request packets, with the relevant accounting information, from the network access server (NAS) to a RADIUS server.

Note The RADIUS accounting requests send data, such as VLAN ID, authentication methods, and so on, to a session.

RADIUS accounting covers the following updates:

- **Interim Updates**: When RADIUS accounting covers DHCP_TLVs, HTTP_TLVs, IP, or ROAM (state machine) changes, the updates are referred to as interim updates or interim accounting.
- **Periodic Updates**: When RADIUS accounting is specified by a timer value, the updates are referred to as periodic updates.

Note Disable the interim updates for the following reasons:

- They cause unnecessary traffic to be sent.
- They drive up error rates.
- They impact alarm thresholds and other metrics that are used for venue-authentication performance.

By default, the Interim Accounting feature is enabled with the **aaa accounting Identity default start-stop group radius** command.

Disabling Interim Accounting (CLI)

Before you begin

You must disable the Policy Profile before performing this procedure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**no accounting-interim** **Example:** `Device(config-wireless-policy)# no accounting-interim`	Disables interim accounting.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Verifying Interim Accounting

To verify the interim accounting updates, run the following command:

```
Device# show wireless profile policy detailed default-policy-profile | s Interim
Interim Accounting Updates: DISABLED
```



CHAPTER 76

Wireless Multicast

- Information About Wireless Multicast, on page 829
- Prerequisites for Configuring Wireless Multicast, on page 832
- Restrictions on Configuring Wireless Multicast, on page 833
- Configuring Wireless Multicast, on page 833
- IPv6 Multicast-over-Multicast, on page 835
- Directed Multicast Service, on page 838
- Wireless Broadcast, Non-IP Multicast and Multicast VLAN, on page 840
- Multicast Filtering, on page 846

Information About Wireless Multicast

If the network supports packet multicasting, the multicast method that the controller uses can be configured. The controller performs multicast routing in two modes:

- Unicast mode: The controller unicasts every multicast packet to every access point associated to the controller. This mode is inefficient and generates a lot of extra traffic in the device and the network, but is required on networks that do not support multicast routing (needed if the APs are on different subnets than the device's wireless management interface).
- Multicast mode: The controller sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the controller processor and shifts the work of packet replication to the network, which is much more efficient than the unicast method.

The FlexConnect mode has two submodes: local switching and central switching. In local switching mode, the data traffic is switched at the AP level and the controller does not see any multicast traffic. In central switching mode, the multicast traffic reaches the controller. However, IGMP snooping takes place at the AP.

When the multicast mode is enabled and the controller receives a multicast packet from the wired LAN, the controller encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The controller always uses the management VLAN for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the VLAN on which clients receive multicast traffic.

The controller supports all the capabilities of IGMP v1, including Multicast Listener Discovery (MLD) v1 snooping, but the IGMP v2 and IGMP v3 capabilities are limited. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, global multicast mode should be enabled.

Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, the controller snooping gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) based on the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the IGMP querier. The controller then updates the access-point MGID table on the corresponding access point with the client MAC address. When the controller receives multicast traffic for a particular multicast group, it forwards it to all the access points, but only those access points that have active clients listening or subscribed to that multicast group send multicast traffic on that particular WLAN. IP packets are forwarded with an MGID that is unique for an ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID that is unique for the ingress VLAN.

MGID is a 14-bit value filled in the 16-bit reserved field of wireless information in the CAPWAP header. The remaining two bits should be set to zero.

Multicast Optimization

Multicast optimization enables you to create a multicast VLAN that can be used for multicast traffic. One of the VLANs in the device can be configured as a multicast VLAN where multicast groups are registered. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the multicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The device makes sure that all the multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.

Note When VLAN groups are defined and uses multicast communication, then you need to enable the multicast VLAN.

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are IPv6 global policies features. Every time an ND inspection is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 RA guard is enabled by default on the controller. RA from the wired side should be forwarded to the wireless clients if the Stateless Address Auto-Configuration (SLAAC) is deployed in the network.

Information About IPv6 Snooping

The following sections provide information about IPv6 snooping.

IPv6 Neighbor Discovery Inspection

The IPv6 Neighbor Discovery Inspection, or IPv6 snooping feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 Address Glean and IPv6 Device Tracking. IPv6 neighbor discovery (ND) inspection operates at Layer 2, or between Layer 2 and Layer 3, and provides IPv6 features with security and scalability. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism,

such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped. An ND message is considered trustworthy if its IPv6-to-MAC mapping is verifiable. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

When IPv6 ND inspection is configured on a target (which varies depending on platform target support and may include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the ND protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic up to the switch integrated security features (SISF) infrastructure in the routing device. For ND traffic, messages such as NS, NA, RS, RA, and REDIRECT are directed to SISF. For DHCP, UDP messages sourced from port 546 or 547 are redirected.

IPv6 ND inspection registers its "capture rules" to the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL down into the platform-dependent modules. Upon receiving redirected traffic, the classifier calls all entry points from any registered feature (for the target on which the traffic is being received), including the IPv6 ND inspection entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 ND inspection decision.

IPv6 Device Tracking

IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 First-Hop Security Binding Table

The IPv6 First-Hop Security Binding Table recovery mechanism feature enables the binding table to recover in the event of a device reboot. A database table of IPv6 neighbors connected to the device is created from information sources such as ND snooping. This database, or binding, table is used by various IPv6 guard features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

This mechanism enables the binding table to recover in the event of a device reboot. The recovery mechanism will block any data traffic sourced from an unknown source; that is, a source not already specified in the binding table and previously learned through ND or DHCP gleaning. This feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. When a failure occurs, a binding table entry is recovered by querying the DHCP server or the destination host, depending on the configuration.

Recovery Protocols and Prefix Lists

The IPv6 First-Hop Security Binding Table Recovery Mechanism feature introduces the capability to provide a prefix list that is matched before the recovery is attempted for both DHCP and NDP.

If an address does not match the prefix list associated with the protocol, then the recovery of the binding table entry will not be attempted with that protocol. The prefix list should correspond to the prefixes that are valid for address assignment in the Layer 2 domain using the protocol. The default is that there is no prefix list, in which case the recovery is attempted for all addresses. The command to associate a prefix list to a protocol is **protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*].

IPv6 Address Glean

IPv6 address glean is the foundation for many other IPv6 features that depend on an accurate binding table. It inspects ND and DHCP messages on a link to glean addresses, and then populates the binding table with these addresses. This feature also enforces address ownership and limits the number of addresses any given node is allowed to claim.

The following figure shows how IPv6 address glean works.

Figure 21: IPv6 Address Glean



Prerequisites for Configuring Wireless Multicast

- To participate in IP multicasting, the multicast hosts, routers, and multilayer switches must have IGMP operating.
- When enabling multicast mode on the controller, a CAPWAP multicast group address should also be configured. Access points listen to the CAPWAP multicast group using IGMP.

- You must be cautious when using IGMPv3 with switches that are enabled for IGMP snooping. The IGMPv3 messages are different from the messages used in IGMP Version 1 (IGMPv1) and Version 2 (IGMPv2). If your switch does not recognize IGMPv3 messages, the hosts do not receive traffic when IGMPv3 is used.

  IGMPv3 devices do not receive multicast traffic in either cases:

  - When IGMP snooping is disabled.
  - When IGMPv2 is configured on the interface.

  It is recommended to enable IGMPv3 on all intermediate or other Layer 3 network devices. Primarily, on each subnet used by multicast devices including controller and AP subnets.

Restrictions on Configuring Wireless Multicast

The following are the restrictions for configuring IP multicast forwarding:

- Access points in monitor mode, sniffer mode, or rogue-detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the controllers should be different for different controllers.
- Multicast routing should not be enabled for the management interface.
- Multicast with VLAN group is only supported in local mode AP.
- Multicast traffic from wireless clients in non-multicast VLAN should be routed by the uplink switch.
- Multicast traffic on an AAA overridden VLAN is not supported.

Restrictions for IPv6 Snooping

The IPv6 snooping feature is not supported on EtherChannel ports.

Configuring Wireless Multicast

The following sections provide information about the various wireless multicast configuration tasks:

Configuring Wireless Multicast-MCMC Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**wireless multicast***ip-addr* **Example:** `Device(config)# wireless multicast 231.1.1.1`	Enables multicast-over-multicast. Use the **no** form of this command to disable the feature.

	Command or Action	Purpose
Step 2	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Wireless Multicast-MCUC Mode

Note The wireless multicast to unicast (MCUC) mode is only supported in 9800-CL small template.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** **Example:** `Device(config)# wireless multicast`	Enables the multicast traffic for wireless clients.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Multicast Listener Discovery Snooping (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 Click **MLD Snooping**.

Step 3 In the **MLD Snooping** section, click the toggle button to enable or disable MLD snooping.

Step 4 Enter the **MLD Query Interval**, in milliseconds. The value range is between 100 ms and 32767 ms. The default value is 1000 ms.

Step 5 Move the required VLAN IDs listed in the **Disabled** section to the **Enabled** section. (By default, this feature is disabled on the VLAN.)

You can also search for a VLAN ID using the search field. You can click **Disable All** to move all the VLAN IDs from the **Enabled** list to the **Disabled** list, or click **Enable All** to move all the VLAN IDs from the **Disabled** list to the **Enabled** list.

Step 6 Click **Apply to Device**.

Configuring IPv6 MLD Snooping

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# ipv6 mld snooping`	Enters global configuration mode.
Step 2	**ipv6 mld snooping** **Example:** `Device(config)# ipv6 mld snooping`	Enables MLD snooping.

Verifying the Multicast VLAN Configuration

To view the multicast VLAN associated with a policy profile along with the VLAN assigned to that profile, use the following command:

```
Device# show wireless profile policy detail default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : vlan-pool1
Multicast VLAN        : 84
Client count                  : 0
Passive Client                : DISABLED
```

To view the multicast VLAN associated with a client, use the following command:

```
Device# show wireless client mac ac2b.6e4b.551e detail

Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 84.84.0.20
…….
VLAN : 82
Access VLAN : 82
Multicast VLAN: 84
```

IPv6 Multicast-over-Multicast

IPv6 multicast allows a host to send a single data stream to a subset of all the hosts (group transmission) simultaneously. When IPv6 Multicast over Multicast is configured, all the APs join the IPv6 multicast address, and the multicast traffic from the wireless controller to the AP flows over the IPv6 multicast tunnel.

In mixed deployments (IPv4 and IPv6), the APs might join the wireless controller over IPv4 or IPv6. To enable Multicast over Multicast in mixed deployments, configure both IPv4 and IPv6 multicast tunnels. The IPv4 APs have a unicast IPv4 CAPWAP tunnel and join the IPv4 multicast group. The IPv6 APs will have a unicast IPv6 CAPWAP tunnel and joins the IPv6 multicast group.

Note Mixed mode of Multicast over Unicast and Multicast over Multicast over IPv4 and IPv6 is not supported in Cisco IOS XE Gibraltar 16.10.1.

Table 58: Multicast Support Per Platform

Platform	Multicast Support - Multicast over Unicast	Multicast Support - Multicast over Multicast
Cisco Catalyst 9800-40 Wireless Controller	No	Yes
Cisco Catalyst 9800-80 Wireless Controller	No	Yes
Cisco Catalyst 9800 Wireless Controller for Cloud - Small Template	Yes	Yes
Cisco Catalyst 9800 Wireless Controller for Cloud - Medium Template	No	Yes
Cisco Catalyst 9800 Wireless Controller for Cloud - Large Template	No	Yes
Cisco Catalyst 9800-L Wireless Controller	Yes	Yes

Configuring IPv6 Multicast-over-Multicast (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 From the **AP Capwap Multicast** drop-down list, select **Multicast**.

Step 3 Enter the **AP Capwap IPv6 Multicast group Address**.

Step 4 Click **Apply**.

Configuring IPv6 Multicast-over-Multicast

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** {*ipv4-address* | **ipv6** *ipv6-address*) **Example:** `Device(config)# wireless multicast ipv6 ff45:1234::86`	Configures IPv6 multicast-over-multicast address.

Verifying IPv6 Multicast-over-Multicast

To verify the IPv6 multicast-over-multicast configuration, use the following commands:

```
Device# show wireless multicast

Multicast : Enabled
AP Capwap Multicast : Multicast
AP Capwap IPv4 Multicast group Address : 231.1.1.1
AP Capwap IPv6 Multicast group Address : ff45:1234::86
Wireless Broadcast : Disabled
Wireless Multicast non-ip-mcast : Disabled


Device# show running-configuration | inc multicast

show run | inc multicast:--

wireless multicast
wireless multicast ipv6 ff45:1234::86
wireless multicast 231.1.1.1
```

Verifying the Multicast Connection Between the Controller and the AP

Cisco Catalyst 9800 Series Wireless Controller initiates a ping request that passes through the CAPWAP multicast tunnel onto the CAPWAP multicast receiver, which is the AP. In response, the AP pings the packets for CAPWAP multicast group IP address, and sends back the response to the controller. You can view the statistics on the AP for transmitted and received traffic to analyze the data that are sent and received through the multicast tunnel. Alternatively, you can also verify by enhancing the existing statistics on the AP for transmitted and received traffic to explicitly list the joins, leaves, data packets transmitted and received through the multicast tunnel.

To confirm if the APs receive multicast to multicast (mom) traffic sent by the controller, use the following command

```
Device# show ap multicast mom

AP Name                    MOM-IP     TYPE MOM- STATUS
```

```
-----------------------------------------------------
SS-E-1                      IPv4             Up
SS-E-2                      IPv4             Up
9130E-r3-sw2-g1012          IPv4             Up
9115i-r3-sw2-te1-0-38       IPv4             Up
AP9120-r3-sw3-Gi1-0-46      IPv4             Up
ap3800i-r2-sw1-te2-0-2      IPv4             Up
```

Directed Multicast Service

The Directed Multicast Service (DMS) feature allows a client to request access points (AP) to transmit multicast packets as unicast frames. After receiving this request, an AP buffers the multicast traffic for a client and transmits it as a unicast frame when the client wakes up. This allows the client to receive the multicast packets that were ignored while in sleep mode (to save battery power) and also ensures Layer 2 reliability. The unicast frames are transmitted to the client at a potentially higher wireless link rate, which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus saving more battery power. Without DMS, the client has to wake up at each Delivery Traffic Indication Map (DTIM) interval to receive multicast traffic.

Configuring Directed Multicast Service(GUI)

Procedure

Step 1 Choose **Configuration > Wireless > WLANs > Wireless Networks**.

Step 2 Select a **WLAN** to view the **Edit WLAN** window.

Step 3 Click **Advanced** tab.

Step 4 Check the **Directed Multicast Service** check box to enable the feature.

Step 5 Click **Update & Apply to Device**.

Configuring Directed Multicast Service

Before you begin

- This feature is enabled on receiving a request from a client. Ensure that this feature is configured under WLAN.
- This feature is supported only on 802.11v-capable clients, such as Apple iPad and Apple iPhone.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test5`	Configures the WLAN profile and enters WLAN profile configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN profile.
Step 4	**dms** **Example:** `Device(config-wlan)# dms`	Configures DMS processing per WLAN.
Step 5	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN profile.

Verifying the Directed Multicast Service Configuration

To verify the status of the DMS configuration on the controller, use **show** commands below. The DMS status is displayed under *IEEE 802.11v Parameters*.

```
Device# show wlan id 5

WLAN Profile Name     : test
================================================
Identifier                                      : 5
Network Name (SSID)                             : test
Status                                          : Disabled
Broadcast SSID                                  : Enabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
!
.
.
.
Assisted-Roaming
    Neighbor List                               : Disabled
    Prediction List                             : Disabled
    Dual Band Support                           : Disabled

! DMS status is displayed below.

IEEE 802.11v parameters
    Directed Multicast Service                  : Enabled
    BSS Max Idle                                : Disabled
        Protected Mode                          : Disabled
    Traffic Filtering Service                   : Disabled
    BSS Transition                              : Enabled
        Disassociation Imminent                 : Disabled
            Optimized Roaming Timer             : 40
            Timer                               : 200
    WNM Sleep Mode                              : Disabled
```

```
802.11ac MU-MIMO                                : Disabled
802.11ax parameters
    OFDMA Downlink                              : unknown
    OFDMA Uplink                                : unknown
    MU-MIMO Downlink                            : unknown
    MU-MIMO Uplink                              : unknown
    BSS Color                                   : unknown
    Partial BSS Color                           : unknown
    BSS Color Code
```

To verify the status of the DMS configuration on the controller for clients, use the following command:

```
Device# show wireless client mac-address 6c96.cff2.83a0 detail | inc 11v

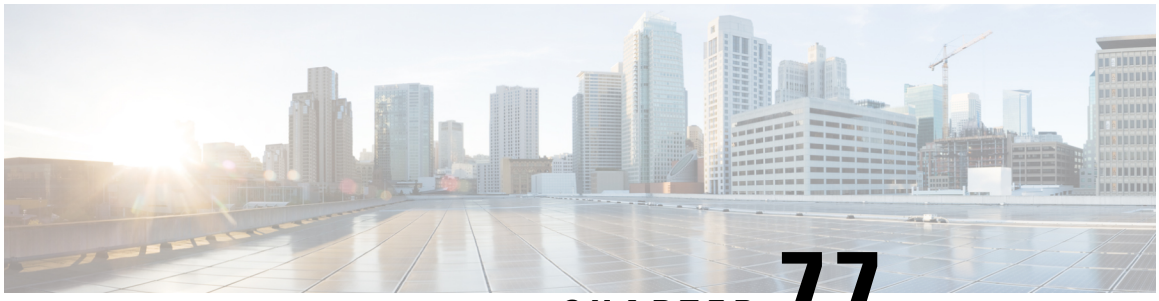
11v BSS Transition : implemented
11v DMS Capable : Yes
```

To verify the DMS request and response statistics, use the following command:

```
Device# show wireless stats client detail | inc DMS

Total DMS requests received in action frame      : 0
Total DMS responses sent in action frame         : 0
Total DMS requests received in Re-assoc Request  : 0
Total DMS responses sent in Re-assoc Response    : 0
```

To verify the DMS configuration Cisco Aironet 2700 and 3700 Series APs, use the following command:

```
AP# show controllers dot11Radio 0/1 | begin Global DMS

Global DMS - requests:0 uc:0 drop:408
DMS enabled on WLAN(s): dms-open
 test-open
```

To verify the DMS configuration on the Cisco Aironet 2800, 3800, and 4800 Series APs, use the following command:

```
AP# show multicast dms all

 vapid    client               dmsid        TClas
 0       1C:9E:46:7C:AF:C0     1    mask:0x55, version:4, proto:0x11, dscp:0x0, sport:0,
dport:9, sip:0.0.0.0, dip:224.0.0.251
```

Wireless Broadcast, Non-IP Multicast and Multicast VLAN

Restrictions

- Wireless broadcast does not support VLAN groups.
- When a VLAN pool is mapped to the WLAN profile, support for forwarding non-IPv4 multicast and broadcast is unavailable.
- Non-IPv4 multicasts and broadcasts are restricted to clients on the VLAN mapped to the WLAN and are not forwarded on VLANs returned by AAA override.

Configuring Non-IP Wireless Multicast (CLI)

Before you begin

- The non-IP Multicast feature is disable globally, by default.
- For non-IP multicast, global wireless multicast must be enabled for traffic to pass.
- This feature is not supported in Fabric or Flex deployments.

Procedure

	Command or Action	Purpose
Step 1	**wireless multicast non-ip** **Example:** `Device(config)# wireless multicast non-ip`	Enables non-IP multicast in all the VLANs. By default, the non-IP multicast in all the VLANs is in Disabled state. Wireless multicast must be enabled for the traffic to pass. Use the **no** form of this command to disable non-IP multicast in all the VLANs.
Step 2	**wireless multicast non-ip vlan** *vlanid* **Example:** `Device(config)# wireless multicast non-ip vlan 5`	Enables non-IP multicast per VLAN. By default, non-IP multicast per VLAN is in Disabled state. Both wireless multicast and wireless multicast non-IP must be enabled for traffic to pass. Use the **no** form of this command to disable non-IP multicast per VLAN.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Wireless Broadcast (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 In the Multicast page, change the status of the **Wireless Broadcast** to enabled to broadcast packets for wireless clients.

The default value is disabled.

Step 3 From the Disabled VLAN table, click the arrow adjacent to the VLAN ID in the **Disabled** state to the **Enabled** state to enable broadcast packets for a VLAN.

The default value is disabled.

Step 4 Save the configuration.

Configuring Wireless Broadcast (CLI)

Before you begin

- This feature is applicable only to non-ARP and DHCP broadcast packets.
- This feature is disable globally, by default.
- This feature is not supported in Fabric or Flex deployments.

Procedure

	Command or Action	Purpose
Step 1	**wireless broadcast** **Example:** `Device(config)# wireless broadcast`	Enables broadcast packets for wireless clients. By default, the broadcast packets for wireless clients is in Disabled state. Enabling **wireless broadcast** enables broadcast traffic for each VLAN. Use the **no** form of this command to disable broadcasting packets.
Step 2	**wireless broadcast vlan** *vlanid* **Example:** `Device(config)# wireless broadcast vlan 3`	Enables broadcast packets for single VLAN. By default, the Broadcast Packets for a Single VLAN feature is in Disabled state. Wireless broadcast must be enabled for broadcasting. Use the **no** form of this command to disable broadcast traffic for each VLAN.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring Multicast-over-Multicast for AP Multicast Groups (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap capwap multicast** *IP address* **Example:** `Device(config)# ap capwap multicast 239.4.4.4`	Configures an all-AP multicast group to send a single packet to all the APs.
Step 2	**wireless multicast** *IP address* **Example:** `Device(config)# wireless multicast 239.4.4.4`	Enables Multicast-over-Multicast for multicasting client multicast group traffic to all the APs through the underlying all-AP multicast group. *IP address*—Multicast-over-multicast IP address.

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Verifying Wireless Multicast

Table 59: Commands for Verifying Wireless Multicast

Command	Description
show wireless multicast	Displays the multicast status and IP multicast mode, and each VLAN's broadcast and non-IP multicast status. Also displays the Multicast Domain Name System (mDNS) bridging state.
show wireless multicast group summary	Displays all (Group and VLAN) lists and the corresponding MGID values.
show wireless multicast [**source** *source*] **group** *group* **vlan** *vlanid*	Displays details of the specified (S,G,V) and shows all the clients associated with and their MC2UC status.
show ip igmp snooping wireless mcast-ipc-count	Displays the number of multicast IPCs per MGID sent to the wireless controller module.
show ip igmp snooping wireless mgid	Displays the MGID mappings.
show ip igmp snooping igmpv2-tracking	Displays the client-to-SGV mappings and the SGV-to-client mappings.
show ip igmp snooping querier vlan *vlanid*	Displays the IGMP querier information for the specified VLAN.
show ip igmp snooping querier detail	Displays the detailed IGMP querier information of all the VLANs.
show ipv6 mld snooping querier vlan *vlanid*	Displays the MLD querier information for the specified VLAN.
show ipv6 mld snooping wireless mgid	Displays MGIDs for the IPv6 multicast group.

Multicast Optimization

Multicast used to be based on the group of the multicast addresses and the VLAN as one entity, MGID. With the VLAN group, duplicate packets might increase. Using the VLAN group feature, every client listens to the multicast stream on a different VLAN. As a result, the device creates different MGIDs for each multicast address and the VLAN. Therefore, the upstream router sends a copy for each VLAN, which results in as many copies as the number of VLANs in the group. Because the WLAN remains the same for all the clients, multiple copies of the multicast packet are sent over the wireless network. To suppress the duplication of a multicast stream on the wireless medium between the device and the access points, the multicast optimization feature can be used.

Multicast optimization enables you to create a multicast VLAN that can be used for multicast traffic. One of the VLANs in the device can be configured as a multicast VLAN where multicast groups are registered. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the multicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The device makes sure that all the multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.

Configuring IP Multicast VLAN for WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** and **Description**.

Step 4 Enable the **Central Switching** and **Central Association** toggle buttons.

Step 5 In the **Access Policies** tab, under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list and enter the **Multicast VLAN**.

Step 6 Click **Apply to Device**.

Configuring IP Multicast VLAN for WLAN

Before you begin

- This feature is not supported in Fabric or Flex deployments.
- Multicast VLAN is used for both IPv4 and IPv6 multicast forwarding to APs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 4	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures WLAN for central switching.
Step 5	**description** *policy-profile-name* **Example:** `Device(config-wireless-policy)# description "test"`	(Optional) Adds a description for the policy profile.
Step 6	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.
Step 7	**multicast vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# multicast vlan 84`	Configures multicast for the VLAN.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Verifying the Multicast VLAN Configuration

To view the multicast VLAN associated with a policy profile along with the VLAN assigned to that profile, use the following command:

```
Device# show wireless profile policy detail default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : vlan-pool1
Multicast VLAN        : 84
Client count                  : 0
Passive Client                : DISABLED
```

To view the multicast VLAN associated with a client, use the following command:

```
Device# show wireless client mac ac2b.6e4b.551e detail

Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 84.84.0.20
```

```
.........
VLAN : 82
Access VLAN : 82
Multicast VLAN: 84
```

Multicast Filtering

Information About Multicast Filtering

In Cisco IOS XE Amsterdam, Release 17.2.1, the Multicast Filtering feature is supported on Layer 3 for IPv4.

You can enable or disable the multicast filtering feature per WLAN from the controller. When you enable this feature, the APs drop the Internet Group Management Protocol (IGMP) join request from a client that is part of the WLAN, for any Layer 3 multicast group address. When you disable this feature, the APs honor the IGMP join request from the client that is part of the WLAN.

In the Cisco IOS XE Amsterdam, Release 17.3.1, the Multicast Filtering feature is supported on Layer 3 for IPv6.

You can enable or disable the Multicast Filtering feature per WLAN, from the controller. The following table shows the AP behavior with IPv4 and IPv6:

The Multicast Filtering feature is disabled by default.

Table 60: Multicast Filtering per WLAN

Multicast Filtering Feature Status	IPv4	IPv6
Enabled	AP drops the Internet Group Management Protocol (IGMP) membership report from a client that is a part of a WLAN.	AP drops the Multicast Listener Discovery (MLD) report with multicast group address scope value greater than three, from a client that is a part of a WLAN.
Disabled	AP honors the IGMP membership report from the client that is a part of a WLAN.	AP honors the MLD report from the client that is a part of a WLAN.

Supported L3 Multicast Report for Filtering

APs will not honor and drop IGMP and MLD join requests from a client part of WLAN for any L3 multicast group address as per the below filtering options:

- IPv4: IGMP versions to be filtered:
  - V1 membership report (0x12)
  - V2 membership report (0x16)
  - V3 membership report (0x22)
- IPv6: ICMPv6 types to be filtered, except link-local multicast packets:

- Multicast Listener report: MLD Version 1 (131)
- Multicast Listener report: MLD Version 2 (143)

Note Filtering of supported types will prevent the creation or addition of a client entry to the AP multicast group table.

Configuring Multicast Filtering

Perform the procedure given here to create a policy profile and then enable Multicast Filtering on a WLAN:

Before you begin

Create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**multicast filter** **Example:** `Device(config-wireless-policy)#multicast filter`	Configures a multicast filter. (Use the **no** form of this command to disable the feature.)

What to do next

1. Create a policy tag. For more information about creating policy tags, see *Configuring a Policy Tag (CLI)*.
2. Map the policy tag to an AP. For more information about mapping a policy tag to an AP, see *Attaching a Policy Tag and Site Tag to an AP (CLI)*.

Verifying Multicast Filtering

To verify if multicast filtering is enabled, use the **show wireless profile policy detailed** *named-policy-profile* command:

```
Device# show wireless profile policy detailed  named-policy-profile
Policy Profile Name                : named-policy-profile
```

```
Description                     :
Status                          : DISABLED
VLAN                            : 91
Multicast VLAN                  : 0
OSEN client VLAN                :
Multicast Filter                : ENABLED
```



CHAPTER 77

Map-Server Per-Site Support

- Information About Map Server Per Site Support, on page 849
- Configuring the Default Map Server (GUI), on page 850
- Configuring the Default Map Server (CLI), on page 850
- Configuring a Map Server Per Site (GUI), on page 851
- Configuring a Map Server Per Site (CLI), on page 851
- Creating a Map Server for Each VNID (GUI), on page 852
- Creating a Map Server for Each VNID, on page 852
- Creating a Fabric Profile and Associating a Tag and VNID (GUI), on page 853
- Creating a Fabric Profile and Associating a Tag and VNID (CLI), on page 853
- Verifying the Map Server Configuration, on page 854

Information About Map Server Per Site Support

The Map Server Per Site feature supports per-site map server and the selection of map server based on the client's subnet. This enables the controller to support multiple sites and to segregate each site's traffic.

This feature is applicable to both Enterprise and Guest map servers. For the Layer 2 virtual extensible LAN network identifier-based (L2VNID-based) map server, the appropriate map server should be selected based on the L2 VNID.

The following list shows the map server selection order for AP query and client registration:

- Per-L3 VNID map server
- Per site (ap-group) map server
- Default or global map server

Benefits

Some of the benefits of using Map Server Per Site feature are listed below:

- You can use a single large site with horizontal scaling of the map server and border nodes.
- You can share the controller across multiple sites, with each site can having its own map server and virtual network or VNID and still segment traffic from each site.
- You can share Guest map-server across multiple sites while keeping the Enterprise map-server separate.

- You can use the same SSID across different sites. Within a site, they can belong to a different virtual network domain.

Configuring the Default Map Server (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Fabric**.

Step 2 On the **Fabric** page, click the **Control Plane** tab.

Step 3 In the **Control Plane Name** list, click **default-control-plane**.

Step 4 In the **Edit Control Plane** window that is displayed, click **Add**.

Step 5 Enter the IP address of the map server.

Step 6 Set the **Password Type** as either **Unencrypted** or **AES**.

Step 7 Enter the **Pre Shared Key**.

Step 8 Click **Save**.

Step 9 Click **Update & Apply to Device**.

Configuring the Default Map Server (CLI)

Follow the procedure given below to configure the default map server.

Before you begin

- The global map server is the default map server that is used for both AP query (when an AP joins) as well as for client registration (when a client joins).
- We recommend that you configure map servers in pairs to ensure redundancy because s the LISP control-plane does not support redundancy inherently.
- To share a map server set, create a map server group, which can be shared across site profiles, fabric profiles, Layer 2 and Layer3 VNID, as well with the default map server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless fabric control-plane** *control-plane-name*	Configures the control plane name.

	Command or Action	Purpose
	Example: `Device(config)# wireless fabric control-plane test-map`	If you do not provide a control plane name, the default-control-plane that is auto generated is used.
Step 3	**ip address** *ip-address* **key** *pre-shared-key* **Example:** `Device((config-wireless-cp)#ip address 10.12.13.14 key secret`	Configures IP address and the key for the control plane.

Configuring a Map Server Per Site (GUI)

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** page, click the AP Join Profile name.

Step 3 In the **Edit AP Join Profile** window, click the **CAPWAP** tab.

Step 4 In the **High Availability** tab under **Backup Controller Configuration**, check the **Enable Fallback** check box.

Step 5 Enter the primary and secondary controller names and IP addresses.

Step 6 Click **Update & Apply to Device**.

Configuring a Map Server Per Site (CLI)

Follow the procedure given below to configure per-site MAP server under site-tag.

Before you begin

You can configure map server for each site or each AP group. . If a map server is not configured for each VNID or subnet, per-site map server is used for AP queries and client registration.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless tag site** *site-tag* **Example:** `Device(config)# wireless tag site test-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**fabric control-plane** *map-server-name* **Example:** `Device(config-wireless-site)# fabric control-plane test-map`	Associates a fabric control plane name with a site tag.

Creating a Map Server for Each VNID (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless Plus** > **Fabric** > **Fabric Configuration**.
Step 2 In the **Profiles** tab, click **Add** to add a new Fabric Profile.
Step 3 In the **Add New Profile** window that is displayed, enter a name and description for the profile.
Step 4 Specify the L2 VNID and SGT Tag details.
Step 5 In the **Map Servers** section, specify the IP address and preshared key details for Server 1.
Step 6 Optionally, you can specify the IP address and preshared key details for Server 2.
Step 7 Click **Save & Apply to Device.**

Creating a Map Server for Each VNID

Follow the procedure given below to configure map server for each VNID in Layer 2 and Layer 3 or a map server for a client VNID.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	Choose one of the following: • **wireless fabric name** *vnid-map* **l2-vnid** *l2-vnid* **l3-vnid** *l3vnid* **ip** *network-ip subnet-mask* **control-plane** *control-plane-name*	Configures a map server for each VNID in Layer 2 and Layer 3 or a map server for a client VNID.

	Command or Action	Purpose

	• **wireless fabric name** *vnid-map* **l2-vnid** *l2-vnid* **control-plane** *control-plane-name*
	Example:
	`Device(config)# wireless fabric name test1 l2-vnid 12 l3-vnid 10 ip 10.8.6.2 255.255.255.236 control-plane cp1`
	Example:
	`Device(config)# wireless fabric name test1 l2-vnid 22 control-plane cp1`	

Creating a Fabric Profile and Associating a Tag and VNID (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless** > **Fabric**.

Step 2 In the **Profiles** tab on **Fabric Configuration** page, click **Add** to add a new profile.

Step 3 In the **Add New Profile** window that is displayed, enter a name and description for the profile.

Step 4 Specify the L2 VNID and SGT Tag details.

Step 5 Click **Save & Apply to Device**.

Creating a Fabric Profile and Associating a Tag and VNID (CLI)

Follow the procedure given below to create a fabric profile and associate the VNID to which the client belongs and the SGT tag to this profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile fabric** *fabric-profile-name* **Example:** `Device(config)# wireless profile fabric test-fabric`	Configures a fabric profile.
Step 3	**sgt-tag** *value* **Example:**	Configures an SGT tag.

	Command or Action	Purpose
	`Device(config-wireless-fabric)# sgt-tag 5`	
Step 4	**client-l2-vnid** *vnid* **Example:** `Device(config-wireless-fabric)# client-l2-vnid 10`	Configures a client Layer 2 VNID.

Verifying the Map Server Configuration

Use the following commands to verify the map server configuration:

```
Device# show wireless fabric summary

Fabric Status      : Enabled


Control-plane:
Name                              IP-address        Key                               Status
-------------------------------------------------------------------------------------------
test-map                          10.12.13.14       test1                             Down


Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address             Subnet
Control plane name
-------------------------------------------------------------------------------------------------------

  test1               12             10             10.6.8.9            255.255.255.236
 test2


Device# show wireless fabric vnid mapping

Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address             Subnet      Control
 Plane Name
-------------------------------------------------------------------------------------------------------

  fabric1             1              0              9.6.51.0            255.255.255.0
     map-server-name

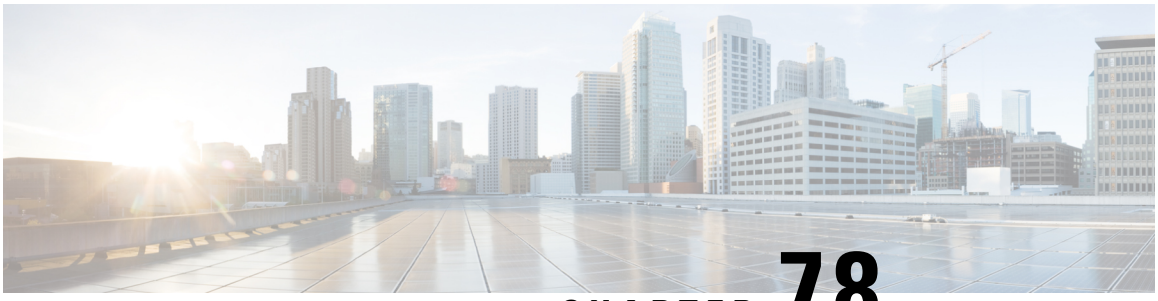
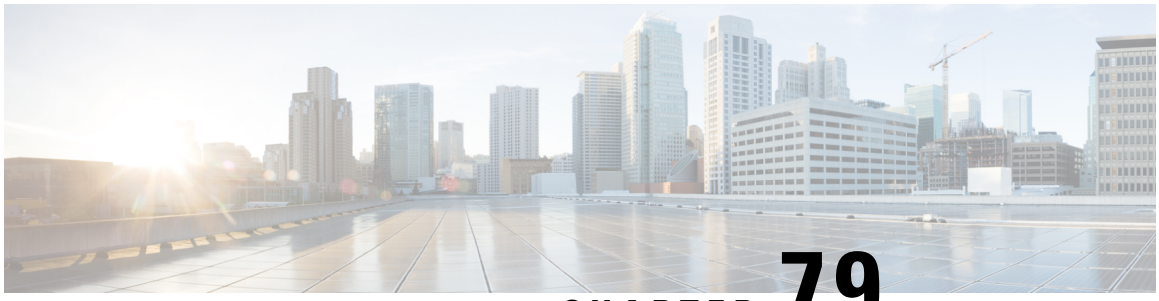
Device# show wireless profile fabric detailed profile-name

Profile-name      : fabric-ap
VNID              : 1
SGT               : 500
Type              : Guest

Control Plane Name       Control-Plane IP   Control-Plane Key
------------------------------------------------------------------------------
 Ent-map-server           5.4.3.2                guest_1

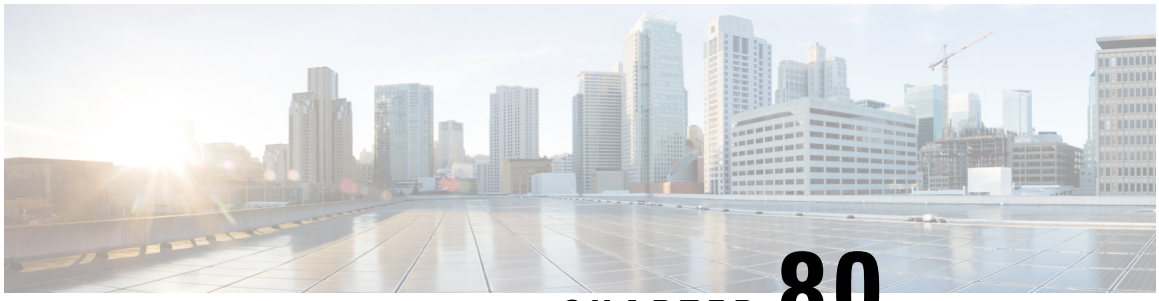
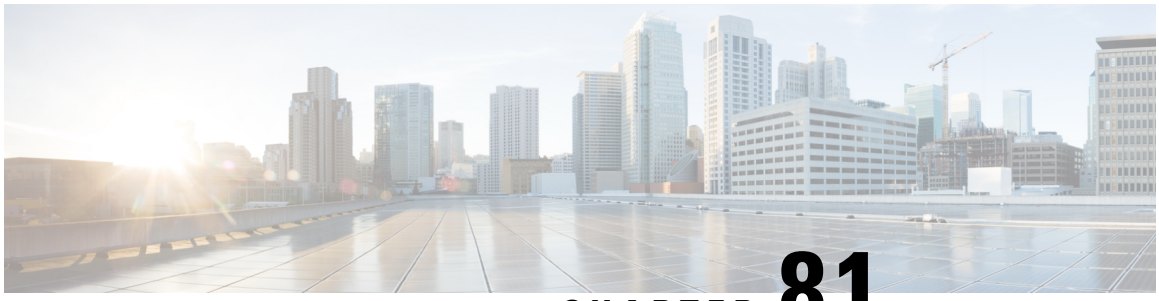
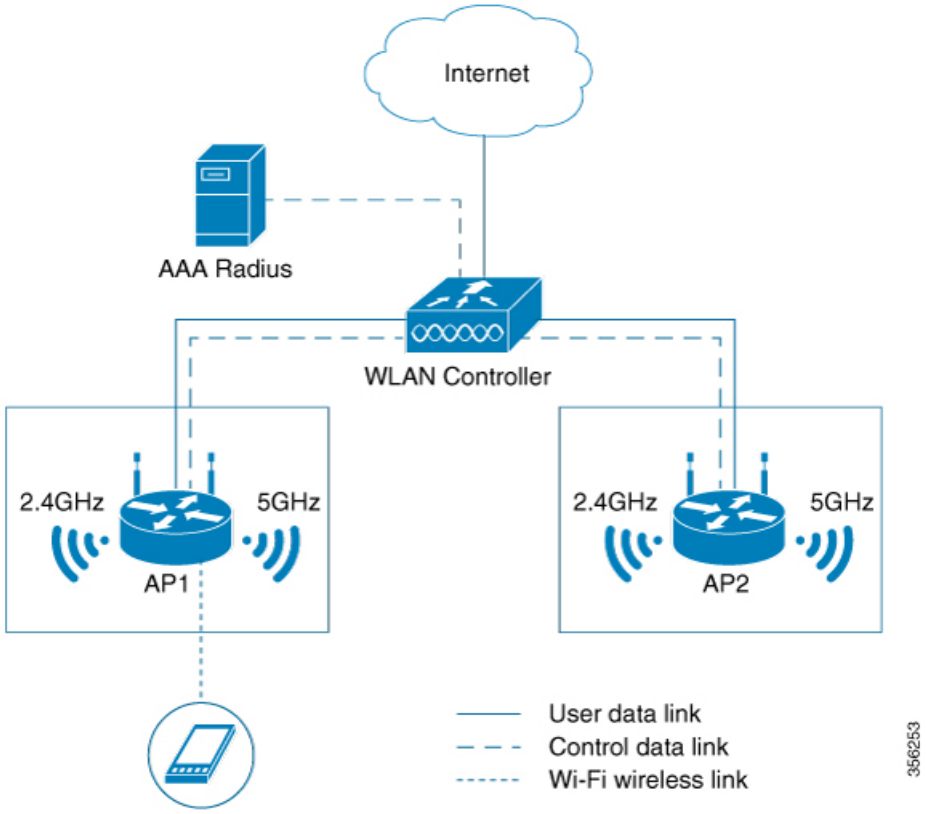
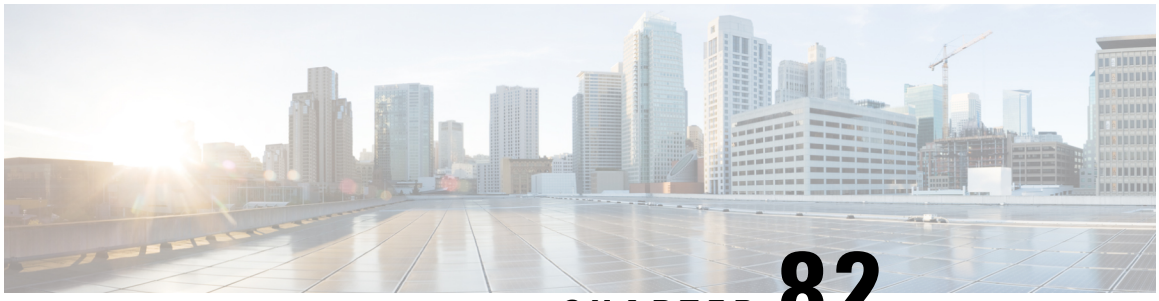
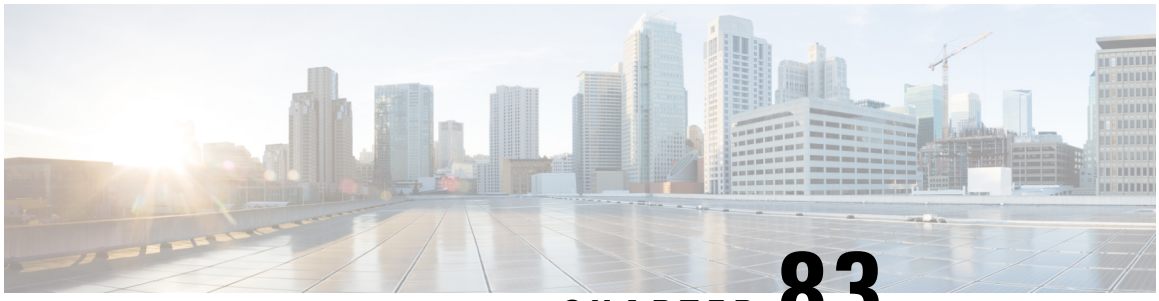
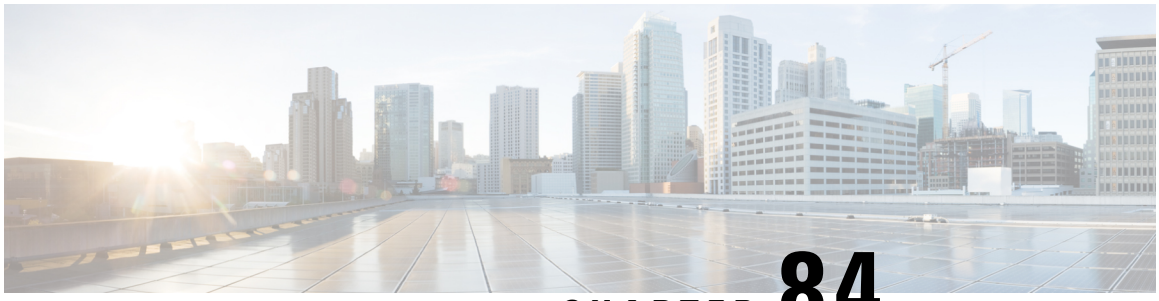
Device# show ap name ap-name config general
```

```
Fabric status                                    : Enabled
RLOC                                             : 2.2.2.2
Control Plane Name  : ent-map-server
```

```
Device# show wireless client mac mac-address detail

Fabric status : Enabled
RLOC                  : 2.2.2.2
Control Plane Name  : ent-map-server
```

```
Device# show wireless tag site detailed site-tag

Site Tag Name        : default-site-tag
Description          : default site tag
---------------------------------------
AP Profile           : default-ap-profile
Local-site           : Yes
Fabric-control-plane: Ent-map-server
```



CHAPTER 78

Volume Metering

- Volume Metering, on page 857
- Configuring Volume Metering, on page 857

Volume Metering

The Volume Metering feature allows you to configure the interval at which an access point (AP) updates client accounting statistics to the controller and in turn to the RADIUS server. Currently, the report is sent from an AP to the controller every 90 seconds. With this feature, you can configure the time from 5 to 90 seconds. This helps reduce the delay in accounting data usage by a device.

Configuring Volume Metering

Follow the procedure given below to configure volume metering:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile yy-ap-profile`	Configures an AP profile and enters ap profile configuration mode.
Step 3	**dot11 24ghz reporting-interval** *reporting-interval* **Example:** `Device(config-ap-profile)# dot11 24ghz reporting-interval 60`	Configures the dot11 parameters.

	Command or Action	Purpose
Step 4	**dot11 5ghz reporting-interval** *reporting-interval* **Example:** `Device(config-ap-profile)# dot11 5ghz reporting-interval 60`	Configures the dot11 parameters.
Step 5	**exit** **Example:** `Device(config-ap-profile)# exit`	Returns to global configuration mode.
Step 6	**aaa accounting update periodic** *interval-in-minutes* **Example:** `Device(config)# aaa accounting update periodic 75`	Sets the time interval (in minutes) at which the controller sends interim accounting updates of the client to the RADIUS server.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits configuration mode and returns to privileged EXEC mode.



CHAPTER 79

Enabling Syslog Messages in Access Points and Controller for Syslog Server

- Information About Enabling Syslog Messages in Access Points and Controller for Syslog Server, on page 859
- Configuring Syslog Server for an AP Profile, on page 861
- Configuring Syslog Server for the Controller (GUI), on page 862
- Configuring Syslog Server for the Controller , on page 863
- Information About Syslog Support for Client State Change, on page 864
- Configuring Syslog Support for Client State Change (CLI), on page 865
- Sample Syslogs, on page 865
- Verifying Syslog Server Configurations, on page 866

Information About Enabling Syslog Messages in Access Points and Controller for Syslog Server

The Syslog server on access points and controller has many levels and facilities.

The following are the Syslog levels:

- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- Notifications
- Informational
- Debugging

The following options are available for the Syslog facility:

- auth—Authorization system.

- cron—Cron/ at facility.
- daemon—System daemons.
- kern—Kernel.
- local0—Local use.
- local1—Local use.
- local2—Local use.
- local3—Local use.
- local4—Local use.
- local5—Local use.
- local6—Local use.
- local7—Local use.
- lpr—Line printer system.
- mail—Mail system.
- news—USENET news.
- sys10—System use.
- sys11—System use.
- sys12—System use.
- sys13—System use.
- sys14—System use.
- sys9—System use.
- syslog—Syslog itself.
- user—User process.
- uucp—Unix-to-Unix copy system.

Note For more information about the usage of the syslog facilities and levels, refer to RFC 5424 *(The Syslog Protocol)*.

Configuring Syslog Server for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters the AP profile configuration mode.
Step 3	**syslog facility** **Example:** `Device(config-ap-profile)# syslog facility`	Configures the facility parameter for Syslog messages.
Step 4	**syslog host** *ip-address* **Example:** `Device(config-ap-profile)# syslog host 9.3.72.1`	Configures the Syslog server IP address and parameters.
Step 5	**syslog level** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} **Example:** `Device(config-ap-profile)# syslog level`	Configures the Syslog server logging level. The following are the Syslog server logging levels: • **emergencies**—Signifies severity 0. Implies that the system is not usable. • **alerts**—Signifies severity 1. Implies that an immediate action is required. • **critical**—Signifies severity 2. Implies critical conditions. • **errors**—Signifies severity 3. Implies error conditions. • **warnings**—Signifies severity 4. Implies warning conditions. • **notifications**—Signifies severity 5. Implies normal but significant conditions. • **informational**—Signifies severity 6. Implies informational messages. • **debugging**—Signifies severity 7. Implies debugging messages.

	Command or Action	Purpose
		Note To know the number of Syslog levels supported, you need to select a Syslog level. Once a Syslog level is selected, all the levels below it are also enabled. If you enable *critical* Syslog level then all levels below it are also enabled. So, all three of them, namely, *critical*, *alerts*, and *emergencies* are enabled.
Step 6	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Syslog Server for the Controller (GUI)

Procedure

Step 1 Choose **Troubleshooting** > **Logs**.

Step 2 Click **Manage Syslog Servers** button.

Step 3 In **Log Level Settings**, from the **Syslog** drop-down list, choose a security level.

Step 4 From the **Message Console** drop-down list, choose a logging level.

Step 5 In **Message Buffer Configuration**, from the **Level** drop-down list, choose a server logging level.

Step 6 In **Size (bytes)**, enter the buffer size. The value can range between 4096 to 2147483647.

Step 7 In **IP Configuration** settings, click **Add**.

Step 8 Choose the **Server Type**, from the **IPv4 / IPv6** or **FQDN** option.

Step 9 For Server Type **IPv4 / IPv6**, enter the **IPv4 / IPv6 Server Address**. For Server Type **FQDN**, enter the **Host Name**, choose the IP type and the appropriate **VRF Name** from the drop-down lists.

To delete a syslog server, click 'x' next to the appropriate server entry, under the **Remove** column.

Note When creating a host name, spaces are not allowed.

Step 10 Click **Apply to Device**.

Note When you click on **Apply to Device**, the changes are configured. If you click on **Cancel**, the configurations are discarded.

Configuring Syslog Server for the Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**logging host** {*hostname* | *ipv6*} **Example:** `Device(config)# logging host 124.3.52.62`	Enables Syslog server IP address and parameters.
Step 3	**logging facility** {**auth** | **cron** | **daemon** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **sys10** | **sys11** | **sys12** | **sys13** | **sys14** | **sys9** | **syslog** | **user** | **uucp**} **Example:** `Device(config)# logging facility syslog`	Enables facility parameter for the Syslog messages. You can enable the following facility parameter for the Syslog messages: • **auth**—Authorization system. • **cron**—Cron facility. • **daemon**—System daemons. • **kern**—Kernel. • **local0** to **local7**—Local use. • **lpr**—Line printer system. • **mail**—Mail system. • **news**—USENET news. • **sys10** to **sys14** and **sys9**—System use. • **syslog**—Syslog itself. • **user**—User process. • **uucp**—Unix-to-Unix copy system.
Step 4	**logging trap** {*severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} **Example:** `Device(config)# logging trap 2`	Enables Syslog server logging level. *severity-level*- Refers to the logging severity level. The valid range is from 0 to 7. The following are the Syslog server logging levels: • **emergencies**—Signifies severity 0. Implies that the system is not usable.

	Command or Action	Purpose
		• **alerts**—Signifies severity 1. Implies that an immediate action is required. • **critical**—Signifies severity 2. Implies critical conditions. • **errors**—Signifies severity 3. Implies error conditions. • **warnings**—Signifies severity 4. Implies warning conditions. • **notifications**—Signifies severity 5. Implies normal but significant conditions. • **informational**—Signifies severity 6. Implies informational messages. • **debugging**—Signifies severity 7. Implies debugging messages. **Note** To know the number of Syslog levels supported, you need to select a Syslog level. Once a Syslog level is selected, all the levels below it are also enabled. If you enable *critical* Syslog level then all levels below it are also enabled. So, all three of them, namely, *critical*, *alerts*, and *emergencies* are enabled.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Information About Syslog Support for Client State Change

When a client joins, dissociates, or rejoins a wireless network, the Syslog Support for Client State Change feature enables you to track client details such as IP addresses, AP names, and so on.

A syslog is generated in the following scenarios:

- When a client moves to RUN state.
- When a client gets a new IP (IPv4 or IPv6) address in the RUN state.
- When a client in RUN state is deleted.

Note When Syslog Support for Client State Change feature is enabled, and the AP moves from standalone to connected, you may observe that usernames are null in **syslog messages and in client detail** for the 802.1X clients associated with that AP. You can ignore this behavior, as it does not have any operational impact. The usernames will get updated after 30 seconds.

Configuring Syslog Support for Client State Change (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless client syslog-detailed** **Example:** `Device(config)# wireless client syslog-detailed`	Enables detailed syslogs for client events.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Sample Syslogs

802.11x Authentication

The following example shows a client IP update:

```
Oct  1 14:41:27.785 IST: %CLIENT_ORCH_LOG-7-CLIENT_IP_UPDATED:
Chassis 1 R0/0: wncd: Username (dev2), MAC: 0062.xxxx.0077,
IP fe80::262:aff:xxxx:77 101.6.2.119 2001:300:8:0:362:aff:xxxx:77 2001:300:8:0:762:aff:xxxx:77

2001:300:8:0:562:aff:xxxx:77 2001:300:8:0:962:aff:xxxx:77 2001:300:8:0:462:aff:xxxx:77
IP address updated, associated to AP (Asim_06-11) with SSID (dev_abcd_wlan_1)
```

The following example shows a client RUN state:

```
Oct  1 14:41:27.779 IST: %CLIENT_ORCH_LOG-7-CLIENT_MOVED_TO_RUN_STATE:
Chassis 1 R0/0: wncd: Username (dev2), MAC: 0062.xxxx.006a, IP 101.xxxx.2.106 associated
to AP
(Asim_06-10) with SSID (dev_abcd_wlan_1)
```

Open Authentication

The following example shows a client IP update:

```
Sep 18 03:22:35.902: %CLIENT_ORCH_LOG-7-CLIENT_IP_UPDATED:
Chassis 1 R0/0: wncd: Username (null), MAC: 6014.xxxx.c5fb, IP 9.9.xxxx.252
fe80::643c:87c1:xxxx:c1c4 IP address updated,
associated to AP (AP2C5A.xxxx.159A) with SSID (test1)
```

The following example shows a client RUN state:

```
Sep 18 03:22:35.257: %CLIENT_ORCH_LOG-7-CLIENT_MOVED_TO_RUN_STATE:
Chassis 1 R0/0: wncd: Username (null), MAC: 6014.xxxx.c5fb, IP 9.9.xxxx.252 associated to
AP (AP2C5A.xxxx.159A) with SSID (test1)
```

The following example shows a client delete state:

```
Sep 18 03:24:45.083: %CLIENT_ORCH_LOG-7-CLIENT_MOVED_TO_DELETE_STATE:
Chassis 1 R0/0: wncd: Username (null), MAC: 6014.xxxx.c5fb, IP fe80::643c:xxxx:e316:c1c4
2001:300:42:0:643c:87c1:xxxx:c1c4
2001:300:42:0:xxxx:82ce:1ae4:5a32 9.9.xxxx.252 disconnected from AP (AP2C5A.xxxx.159A) with
 SSID (test1)
```

Verifying Syslog Server Configurations

Verifying Global Syslog Server Settings for all Access Points

To view the global Syslog server settings for all access points that joins the controller, use the following command:

```
Device# show ap config general
Cisco AP Name : APA0F8.4984.5E48
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
```

```
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone FlexConnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
```

```
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```

Verifying Syslog Server Settings for a Specific Access Point

To view the Syslog server settings for a specific access point, use the following command:

```
Device# show ap name <ap-name> config general
show ap name APA0F8.4984.5E48 config general
Cisco AP Name : APA0F8.4984.5E48
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
```

```
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone FlexConnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```



CHAPTER 80

Login Banner

- Information About Login Banner, on page 871
- Configuring a Login Banner (GUI), on page 871
- Configuring a Login Banner, on page 872

Information About Login Banner

Login banner is used to display a warning or message when you try to login to the controller.

To create a login banner, you must configure a delimiting character that notifies the system that the following text string must be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string for the banner.

Note When HTTP authentication is configured using TACACS+/RADIUS, the banner message does not display on the Web UI.

Configuring a Login Banner (GUI)

Procedure

Step 1 Choose **Administration** > **Device**.

Step 2 In the **General** tab, in the **Banner** field, enter a name for the device and a message.

Step 3 Click **Apply**.

Configuring a Login Banner

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**banner login** *c message c*
	Example:
	`Device(config)# banner login $`
	`Access for authorized users only.`
	`Please enter your username and password.`
	`$`
		Specifies the login message.
		• c— Enters the delimiting character of your choice, for example, a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.
		• message— Enters a login message up to 255 characters. You cannot use the delimiting character in the message.

Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 5	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.



CHAPTER 81

Wi-Fi Alliance Agile Multiband

- Introduction to Wi-Fi Alliance Agile Multiband, on page 873
- Limitations of MBO, on page 875
- Configuring MBO on a WLAN, on page 875
- Verifying MBO Configuration, on page 876

Introduction to Wi-Fi Alliance Agile Multiband

The Wi-Fi Alliance Agile Multiband (MBO) feature enables better use of Wi-Fi network resources. This feature is built on the fundamental premise that both Wi-Fi networks and client devices have information that can enable better roaming decisions and improve the overall performance of Wi-Fi networks and user experience.

Note This feature applies to MBO certified clients only.

This feature certifies the interoperability of a bundle of features that are defined by the IEEE standard amendments 802.11k, 802.11v, and 802.11u, as well as the Wi-Fi-Alliance defined specifications. These technologies are used to exchange access points (AP), band, and channel preferences, link quality, and status information between AP and client device.

MBO focuses on the following:

- Interactions between the wireless clients and APs
- Exchange of AP and client knowledge about the wireless medium (such as RF neighbors)
- Allow clients to work with APs and take intelligent decisions on the connection and improve the quality of service.

Wi-Fi Alliance Agile Multiband Topology

Multiple components form a Wi-Fi Agile Multiband wireless infrastructure network, which may vary based on the wireless network deployment.

The following figure depicts the system topology for connecting Wi-Fi Agile Multiband devices.

Figure 22: Wi-Fi Agile Multiband Wireless Infrastructure Network



The following components form a Wi-Fi Agile Multiband wireless infrastructure network:

- Access Point (AP): A Wi-Fi Agile Multiband wireless infrastructure network contains one or more Wi-Fi Agile Multiband APs.
- WLAN Controller: A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more WLAN controllers that provide centralized management and other features to the interconnected APs.
- Client Station (STA): A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more STAs. These client STAs are single WLAN capable only.
- RADIUS Server: A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more RADIUS Servers that provide Authentication, Authorization, and Accounting (AAA) services.

Supported MBO Components

MBO AP Capability

A new information element is added to the Beacon, Probe Response, Association Response and Re Association Response Frames for 802.11ax APs to inform clients about MBO support.

Note The new information element indicates that Cisco APs are not cellular data aware.

When an SSID is configured on an AP, the MBO AP capability is enabled.

802.11k/v/r Support

One of the prerequisites for MBO is that APs need to support 802.11k/v/r standard-based technologies. Each of the technologies has their own requirements, such as:

- 802.11k – For 802.11k, send the preferred list of AP neighbors to the client upon request and send a beacon request to a client when AP requires a beacon report from the client.
- 802.11v – For 802.11v, steer the client to a less congested AP (not in a MBO client's non-prefer/non-operable channel list that is sent during the association request and/or WNM notification request) using BSS transition.
- 802.11r – The 802.11r MBO-related capabilities are not supported.

802.11u ANQP or GAS Support

For MBO, the 802.11ax APs must have 802.11u ANQP or GAS support.

The following are the prerequisites:

- ANQP responds to the ANQP request for a neighbor report ANQP-element.
- Before authentication, Layer 2 transport needs to be available in the network between a mobile device and server for an advertisement protocol frame.

MBO Beacon Request

Whenever an AP sends a beacon request to the client, the MBO-compliant client responds with a beacon report.

MBO Associate Disallowed IE

Cisco APs include an **Associate Disallowed IE** in their Beacon/Probe response/(Re) association response when they cannot accommodate any new client.

Limitations of MBO

All non-802.11ax access points are not supported.

Configuring MBO on a WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:**	Configures a WLAN and enters the WLAN configuration mode.

	Command or Action	Purpose
	`Device(config)# wlan wlan-demo 1 ssid-demo`	**Note** If you use WPA2 WLAN while configuring MBO for WLAN, you need to enable PMF in your configuration.
Step 3	**mbo** **Example:** `Device(config-wlan)# mbo`	Configures MBO support on WLAN. **Note** Use the **no mbo** command to disable MBO configuration.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying MBO Configuration

To view the MBO configuration, use the following command:

```
Device# show wlan id 1
WLAN Profile Name     : wlan-demo
================================================
Identifier                                       : 1
Description                                      :
Network Name (SSID)                              : ssid-demo
Status                                           : Disabled
Broadcast SSID                                   : Enabled
802.11ax parameters
    OFDMA Downlink                               : Enabled
    OFDMA Uplink                                 : Enabled
    MU-MIMO Downlink                             : Enabled
    MU-MIMO Uplink                               : Enabled
    BSS Color                                    : Enabled
    Partial BSS Color                            : Enabled
    BSS Color Code                               : 0
    BSS Target Wake Up Time                      : Enabled
    BSS Target Wake Up Time Broadcast Support    : Enabled
mDNS Gateway Status                              : Bridge
WIFI Alliance Agile Multiband      : Enabled
```

To view the non-operational or non-preferred channels, use the following command:

```
Device# show wireless client mac-address 3413.e8b5.f252 detail
Client MAC Address : 3413.e8b5.f252
Client IPv4 Address : 192.165.1.53
Client IPv6 Addresses : fe80::98bb:ea89:f016:3332
Client Username: N/A
AP MAC Address : 00ee.ab18.d920
AP Name: ssap-pp
AP slot : 1
Client State : Associated
Policy Profile : prof
Flex Profile : N/A
Wireless LAN Id: 1
WLAN Profile Name: mbo_1
```

```
Wireless LAN Network Name (SSID): mbo_1
BSSID : 00ee.ab18.d92f
Connected For : 25 seconds
Protocol : 802.11ax - 5 GHz
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Session Timeout : 1800 sec (Remaining time: 1779 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : 1.5
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 05/15/2019 16:03:34 IST
Client Join Time:
  Join Time Of Client : 05/15/2019 16:03:34 IST
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 26 seconds
Policy Type : N/A
Encryption Cipher : None
User Personal Network    : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : default
Multicast VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Point of Attachment : capwap_90400001
  IIF ID             : 0x90400001
  Authorized         : TRUE
  Session timeout    : 1800
  Common Session ID: 000000000000000BB92939C5
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
  Server IP :
  Auth Method Status List
  Method : None
  Local Policies:
  Service Template : wlan_svc_prof_local (priority 254)
  VLAN             : 165
  Absolute-Timer   : 1800
  Server Policies:
  Resultant Policies:
```

```
  VLAN Name         : VLAN0165
  VLAN             : 165
  Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Implemented
11v DMS Capable : No
QoS Map Capable : Yes
Non-Preferred Channels : 40
Non-Operable Channels : 56
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received : 0
  Number of Bytes Sent : 0
  Number of Packets Received : 0
  Number of Packets Sent : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -34 dBm
  Signal to Noise Ratio : 56 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : No/Simple client
```



CHAPTER 82

SNMP Traps

- Information About Configuring SNMP Traps, on page 879
- Configuring SNMP Traps (GUI), on page 880
- Enabling Access Points Traps (CLI), on page 880
- Enabling Wireless Client Traps (CLI), on page 881
- Enabling Mesh Traps (CLI), on page 881
- Enabling RF Traps (CLI), on page 882
- Enabling Rogue, Mobility, RRM, and General Traps (CLI), on page 882
- Verifying SNMP Wireless Traps, on page 883

Information About Configuring SNMP Traps

Simple Network Management Protocol (SNMP) Traps are alert messages sent from a remote SNMP-enabled device such as the controller, to an SNMP manager. Traps are unreliable because the receiver does not send acknowledgments when the device receives traps. Hence, the sender cannot determine if the traps were received.

In order to configure the controller to send SNMP notifications, you must enter at least one **snmp-server host** command. If you do not enter an **snmp-server host** command, no notifications are sent.

In order to enable multiple hosts, you must specify separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host. When multiple **snmp-server host** commands are given for the same host and notification of either trap or inform, each command overwrites the previous command. Only the last **snmp-server host** command is taken into account. For example, if you enter an **snmp-server host** inform command for a host and then enter another **snmp-server host** inform command for the same host, the second command replaces the first.

Specify the **snmp-server enable traps wireless <TrapName>** command in order to specify which SNMP notifications are sent globally. In order for a host to receive wireless notifications, at least one **snmp-server enable traps wireless <TrapName>** command and the **snmp-server host** command for that host must be enabled. However, some notification types cannot be controlled with the **snmp-server enable** command. And some notification types are enabled by default . For example, few AP related traps **crash**, **register**, and **noradiocards** are enabled by default.

Configuring SNMP Traps (GUI)

Procedure

Step 1 Choose **Administration** > **Management** > **SNMP**.
The SNMP page is displayed. By default, the SNMP mode is disabled. To enable or disable SMNP, click the **SNMP Mode** toggle button.

Step 2 Choose the **Wireless Traps** tab.
By default, all SNMP wireless traps are disabled except the **Access Point** trap. To enable all the wireless traps, click **Enable All**.

Step 3 Select the wireless SNMP trap that you wish to enable. Click the **Select All** check box to enable all the trapflags present in the trap. For example, to enable all the trapflags in the **Mesh** trap section, check the **Select All** check box present at the right-hand corner of the section. Uncheck the **Select All** check box to remove selection.

Note In the **Access Point** trap, **Crash**, **No Radio Cards**, and **Register** trapflags are enabled by default. Select **Broken Antenna** trapflag to detect broken antenna. Select **AP Stats** trapflag to enable a trap for AP statistics.

Step 4 Click **Apply**.

Enabling Access Points Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps wireless AP** **Example:** `Device# snmp-server enable traps wireless AP`	Enables wireless SNMP traps for access points.
Step 3	**trapflags ap** {**authorization** | **broken-antenna** | **crash** | **interfaceup** | **ipaddrfallback** | **mfp** | **mode** | **noradiocards** | **register**} **Example:** `Device# trapflags ap authorization`	Enables or disables sending AP related trapflags. The **crash**, **noradiocards**, and **register** trapflags are enabled by default.

Enabling Wireless Client Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps wireless bsnMobileStation** **Example:** `Device# snmp-server enable traps wireless bsnMobileStation`	Enables wireless client traps.
Step 3	**trapflags client dot11** {**assocfail** | **associate** | **authenticate** | **authfail** | **deauthenticate** | **disassociate** } **Example:** `Device# trapflags client dot11 assocfail`	Enables or disables dot11 related trapflags for clients.
Step 4	**trapflags client excluded** **Example:** `Device# trapflags client excluded`	Enables the excluded trapflags for clients.

Enabling Mesh Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps wireless MESH** **Example:** `Device# snmp-server enable traps wireless MESH`	Enables wireless mesh traps.
Step 3	**trapflags mesh** {**abate-snr** | **authentication-failure** | **child-moved** |	Enables or disables mesh trapflags.

	Command or Action	Purpose
	excessive-children | **excessive-hopcount** | **onset-snr** | **parent-change** } **Example:** `Device# trapflags mesh abate-snr`	

Enabling RF Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server enable traps wireless bsnAutoRF** **Example:** `Device# snmp-server enable traps wireless bsnAutoRF`	Enables wireless RF related traps.
Step 3	**trapflags rrm-params** { **channels** | **tx-power** } **Example:** `Device# trapflags rrm-params channels`	Enables or disables sending RRM parameter update related traps.
Step 4	**trapflags rrm-profile** { **coverage** | **interference** | **load** | **noise** } **Example:** `Device# trapflags rrm-profile coverage`	Enables or disables RRM profile related traps.

Enabling Rogue, Mobility, RRM, and General Traps (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**snmp-server enable traps wireless rogue** **Example:** `Device# snmp-server enable traps wireless rogue`	Enables traps for wireless rogue.
Step 3	**trapflags rogue-ap** **Example:** `Device# trapflags rogue-ap`	Enables rogue AP detection trapflag.
Step 4	**trapflags rogue-client** **Example:** `Device# trapflags rogue-client`	Enables rogue client detection trapflag.
Step 5	**snmp-server enable traps wireless wireless_mobility** **Example:** `Device# snmp-server enable traps wireless wireless_mobility`	Enables traps for wireless mobility.
Step 6	**trapflags anchor** **Example:** `Device# trapflags anchor`	Enables anchor trapflags.
Step 7	**snmp-server enable traps wireless RRM** **Example:** `Device# snmp-server enable traps wireless RRM`	Enables traps for wireless RRM.
Step 8	**trapflags rrm-params group** **Example:** `Device# trapflags rrm-params group`	Enables or disables the RRM parameter related traps, when the RF manager group changes.
Step 9	**snmp-server enable traps wireless bsnGeneral** **Example:** `Device# snmp-server enable traps wireless bsnGeneral`	Enables general controller traps.

Verifying SNMP Wireless Traps

To verify the various SNMP traps enabled, use the following command:

```
Device# show run | sec trapflag
trapflags ap crash
trapflags ap noradiocards
```

```
trapflags ap register
trapflags rogue-client
```



CHAPTER 83

Disabling Clients with Random MAC Address

- Information About Disabling Clients with Random MAC Addresses, on page 885
- Configuring Random MAC Address Deny (CLI), on page 885
- Verifying Denial of Clients with a Random MAC Address, on page 886

Information About Disabling Clients with Random MAC Addresses

Wireless clients used to associate with a wireless network using the MAC address that is assigned, for the Wi-Fi network interface card (NIC), during manufacture. This globally unique MAC address assigned by the manufacturer is also known as burn-in address (BIA). BIA tracks end users with the help of the MAC address of the Wi-Fi. To improve the privacy of end user products, a locally enabled random MAC address is enabled for Wi-Fi operations.

Prior to Cisco IOS XE Bengaluru 17.5.1 Release, clients joining a wireless network using a random MAC address could not be tracked with ease. From Cisco IOS XE Bengaluru 17.5.1 Release onwards, the controller is equipped with a knob that denies the entry of clients with a random MAC address into the network. When the *local-admin-mac deny* knob is enabled on the controller, the association of a client joining the network with a random MAC address is rejected. By default, this feature is disabled on the controller.

This feature is not supported in Cisco Wave 1 access points.

Configuring Random MAC Address Deny (CLI)

To stop the entry of clients with a random MAC addresses from joining a wireless network, enable the random MAC address deny knob, by following the steps given below.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *wlan-profile-name <1-4096> SSID-network-name* **Example:** `Device(config)# wlan wlan-profile-name 8 ssid-network-name`	Configures the WLAN policy profile.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Shuts down the WLAN.
Step 4	**[no] local-admin-mac deny** **Example:** `Device(config-wlan)# local-admin-mac deny`	Enables the random MAC address deny knob. Use the **no** form of this command to disable the feature.
Step 5	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Device(config-wlan)# end`	Saves the configuration, exits the configuration mode, and returns to privileged EXEC mode.

Verifying Denial of Clients with a Random MAC Address

To verify the denial of a client with a random MAC address, run the **show wlan name** *wlan-profile-name* | **begin locally** command:

```
Device# show wlan name laa | begin locally
Locally Administered Address Configuration
Deny LAA clients                          : Enabled
```

To verify if a client address is a random MAC address, run the **show wireless client mac-address** *MAC-address* **detail** command:

```
Device# show wireless client mac-address 72xx.38xx.2axx detail
Client MAC Address : 72xx.38xx.2axx
Client MAC Type    : Locally Administered Address
Client IPv4 Address      : 9.1.1.1
Client IPv6 Addresses    : fexx::71xx:27xx:a7xx:efxx
Client Username          : 72xx.38xx.2axx
```

To verify how many random MAC clients are present in the system, run the **show wireless stats client detail** command:

```
Device# show wireless stats client detail
Client Summary
------------------------------
Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
Foreign Clients : 0
```

```
Anchor Clients  : 0
Local Clients   : 1
Idle Clients    : 0
Locally Administered MAC Clients: 1
```

To display the statistics of a specific client, run the **show wlan id** *<1-4096>* **client stats** command:

```
Device# show wlan id 8 client stats
Wlan Profile Name: wlan-profile, Wlan Id: 8
Current client state statistics:
------------------------------------------------------------------------------
  Authenticating         : 0
  Mobility               : 0
  IP Learn               : 0
  WebAuth Pending        : 0
  Run                    : 1
Locally Administered MAC Clients         : 1
```

Note Run the **show configuration wlan wlan-name** command on an AP, to view the status of the locally administered address (LAA) on the WLAN.



CHAPTER 84

Dataplane Packet Logging

- Information About Dataplane Packet Logging, on page 889
- Enabling or Disabling Debug Level (CLI), on page 890
- Enabling Packet Logging in Global and Filtered Buffer in Ingress Path (CLI), on page 890
- Enabling Packet Logging in Global and Filtered Buffer in Punt-Inject Path (CLI), on page 891
- Verifying Dataplane Packet Logging, on page 892
- Clearing Logs and Conditions in Global and Filtered Trace Buffers, on page 893

Information About Dataplane Packet Logging

While onboarding wireless clients, you might encounter problems arising from client IP address allocation, Address Resolution Protocol (ARP) resolution, and so on, which require debugging. For rapid debugging of such issues on the controller, the Dynamic Host Configuration Protocol (DHCP), Neighbor Discovery, and ARP packets that go to and from the wireless clients are unconditionally logged.

Packet-logging serviceability captures connectivity information related to wireless clients. Serviceability is divided into the following categories:

- **Global Trace Log**: Global trace logging is a mechanism to capture client connectivity information, and is enabled by default.
- **Filtered Trace Log**: To start packet logging on a filtered trace buffer, you must enable filters using **debug** commands. Filters capture only the specific packet type or the packets based on the MAC address of the clients.

The following are the features of packet logging:

- In addition to DHCP, Neighbor Discovery, and ARP packets, you can also add or remove other packet capture filters.
- Display filters are set to pick a subset of logged packets.
- Packet-logging data provides information such as the client MAC address, client IP address, VLAN, interface, packet type and time delta, that is required for debugging.

Enabling or Disabling Debug Level (CLI)

To enable or disable debug information for global and filtered logic, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**[no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level** {**all** | **error** | **info** | **trace** | **warning**} **Example:** `Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level all`	Enables the debug level information for global and filtered logic. Use the **no** form of this command to disable the feature.

Enabling Packet Logging in Global and Filtered Buffer in Ingress Path (CLI)

To enable packet logging in global and filtered buffer in the ingress path, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**[no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace** **Example:** `Device# [no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace`	Enables the Quantum Flow Processor on global trace buffer in the ingress path. Use the **no** form of this command to disable the feature.
Step 3	**[no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer**	Enables the condition for CAPWAP to log packet information to the filtered trace buffer.

	Command or Action	Purpose
	ingress filtered-trace capwap {**ipv4** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **keepalive**} **Example:** `Device# [no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace capwap ipv4 209.165.200.224/27`	Use the **no** form of this command to disable the feature.
Step 4	**[no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace wlclient** {**ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H*} **Example:** `Device# [no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace wlclient 1pv6-nd`	Enables the condition to log packet information of the wireless client to the filtered trace buffer. Use the **no** form of this command to disable the feature.

Enabling Packet Logging in Global and Filtered Buffer in Punt-Inject Path (CLI)

To enable packet logging in global and filtered trace buffer in the punt-inject path, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**[no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace** **Example:** `Device# [no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace`	Enables the Quantum Flow Processor in global trace buffer in the punt-inject path. Use the **no** form of this command to disable the feature.
Step 3	**[no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace capwap** {**ipv4** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **keepalive**} **Example:**	Enables the condition for CAPWAP to log packet information to the filtered trace buffer in the punt-inject path. Use the **no** form of this command to disable the feature.

	Command or Action	Purpose
	`Device# [no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace capwap ipv4 209.165.200.224/27`	
Step 4	**[no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace wlclient** {**ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H*} **Example:** `Device# [no] debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace wlclient 1pv6-nd`	Enables the condition to log packet information of the wireless client to the filtered trace buffer, in the punt-inject path. Use the **no** form of this command to disable the feature.

Verifying Dataplane Packet Logging

To show trace buffer-configured conditions, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless trace-buffer ingress
conditions
LogTrace Event: Enabled
Trace wlclient-MACs:
    8c85.90ee.ca92
allow_all_AP_kalives: enabled
AP_kalive cnt=1, AP_kalive6 cnt=0
  IP0: 49.1.0.73
```

To view all the log entries in the filtered trace buffer, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless trace-buffer ingress
filtered-trace all
Trace wlclient-MACs: 8c85.90ee.ca92
  Trace-Buffer for Ingress: Enabled
  Total allocated global-log buffer: 16384
  Total allocated filtered-log v=buffers: 4096

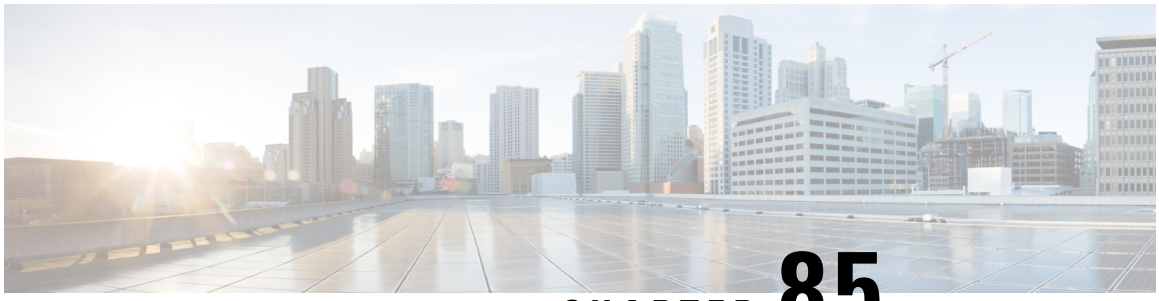
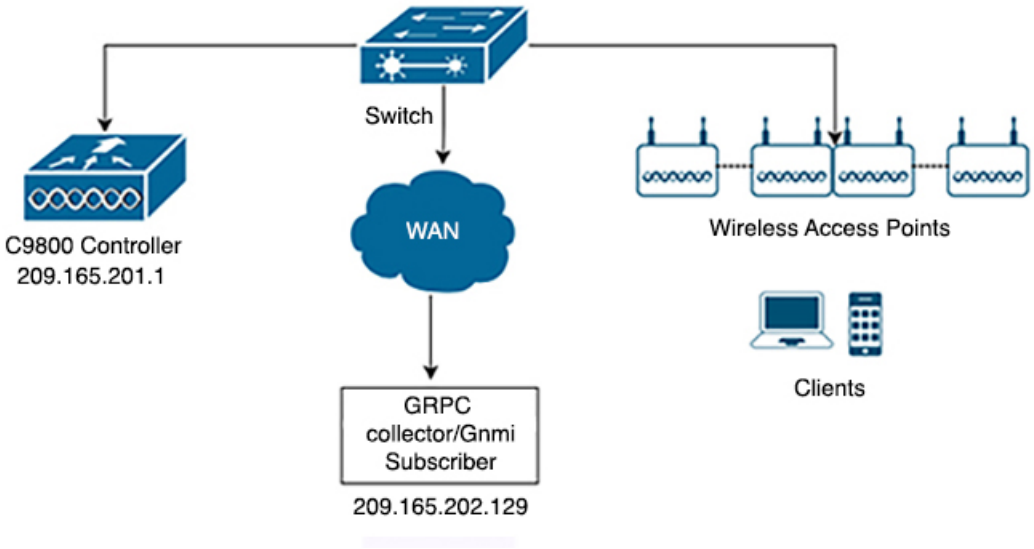
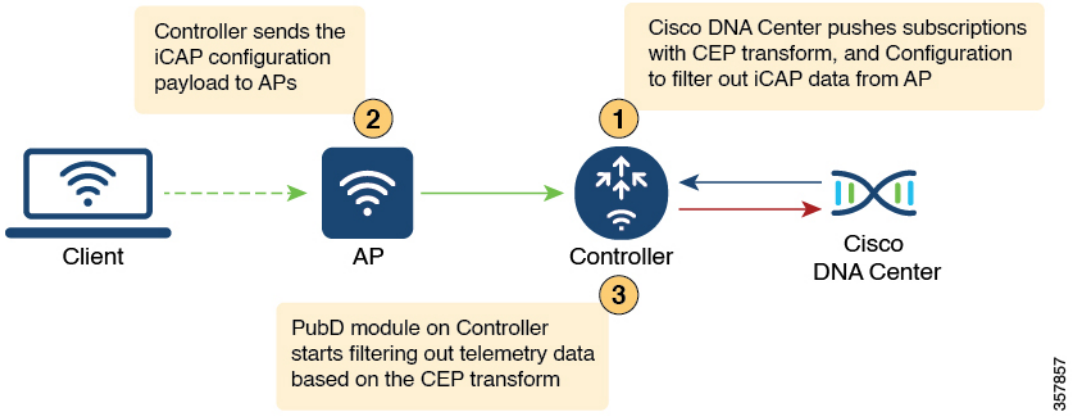
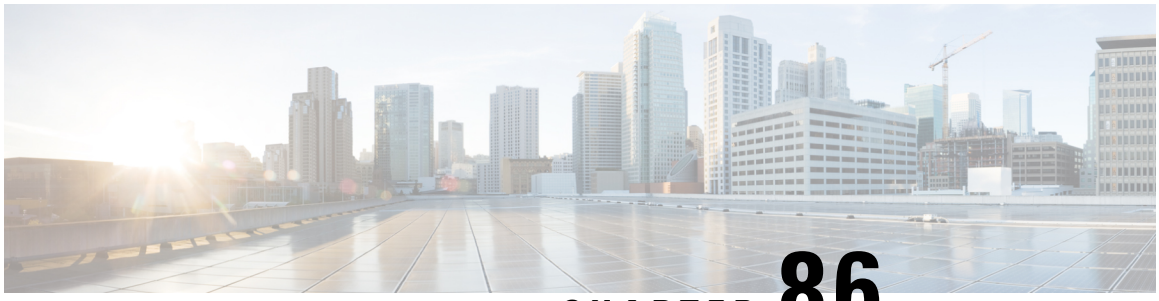
<0 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213207
c=0
<1 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213236
c=0
<2 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213264
c=0
<3 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213293
c=0
<4 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213321
c=0
<5 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213350
c=0
```

To view the number of entries based on a count, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless trace-buffer ingress
filtered-trace 3
Trace wlclient-MACs: 8c85.90ee.ca92
  Trace-Buffer for Ingress: Enabled
  Total allocated global-log buffer: 16384
```

```
  Total allocated filtered-log v=buffers: 4096

<18 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213720
c=0
<19 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213748
c=0
<20 KEEP_ALIVE: CAPWAP peer=49.1.0.73 udp=5256 local=49.1.1.2 udp=5247 vlan=49, dt=213777
c=0

>> 3 entries displayed
   21 entries found in filtered-log buffer
   21 entries ever collected for filtered-log buffer
```

Clearing Logs and Conditions in Global and Filtered Trace Buffers

To clear conditions and logs in the global and filtered trace buffers, use the following commands:

```
Device# clear platform hardware chassis active qfp feature wireless trace-buffer ingress
all
Trace, clear all trace configuration & buffer.

Device# clear platform hardware chassis active qfp feature wireless trace-buffer ingress
conditions
Trace, clear trace configuration

Device# clear platform hardware chassis active qfp feature wireless trace-buffer ingress
filtered-trace
Trace, clear trace Q

Device# clear platform hardware chassis active qfp feature wireless trace-buffer ingress
global-trace
Trace, clear trace global Q
```



CHAPTER 85

Streaming Telemetry

- Information About Streaming Telemetry , on page 895
- Gather Points, on page 895
- Subscription, on page 896
- Transport , on page 897
- Scale Considerations , on page 897
- Session, on page 897
- Configuring Telemetry on a Cisco Catalyst 9800 Series Wireless Controller, on page 898
- On-Change Telemetry Support , on page 905
- Supported XPaths for On-Change Subscription, on page 905
- Troubleshooting Telemetry Support, on page 909
- Cisco Catalyst Center Client Event and SSID Telemetry Filter, on page 911

Information About Streaming Telemetry

Streaming telemetry is a new paradigm in monitoring the health of a network. It provides a mechanism to efficiently stream configuration and operational data of interest from the Cisco Catalyst 9800 Series Wireless Controller. This streamed data is transmitted in a structured format to remote management stations for monitoring and troubleshooting purposes.

This topic explains how to enable the telemetry support the Wi-Fi and system health-related data. Not that telemetry support can be enhanced up to a scale of 1000 access points (APs) and 15000 clients. A single collector setup can be used to subscribe to the requested XPaths. A telemetry feed can be used to subscribe to data elements to monitor APs and clients effectively. Data is provided through the native Cisco wireless models.

Gather Points

Gather points are the top-level XPaths and act as the smallest unit of data exported by a target. Any subscription to an XPath raises to the level of the Gather point, and the target sends updates comprising of all the leaves defined under this Gather point. For example, when you subscribe to an XPath */access-point-operdata/radio-oper-data/vap-oper-config/ssid*, which is part of the Gather point */access-point-operdata/radio-oper-data/vap-oper-config*, the reply will comprise of all the attributes that are a part of the Gather point, in this case, AP-VAP-ID, SSID, and WLAN ID.

The following lists the supported Gather points for an XPaths.

Table 61: Supported Gather Points and Subscription Intervals

Supported Gather Point	Subscription Interval
wireless-access-point-oper:access-point-oper-data/ethernet-mac-wtp-mac-map	>=15 mins
/wireless-access-point-oper:access-point-oper-data/capwap-data	>=15 mins
/wireless-access-point-oper:access-point-oper-data/cdp-cache-data/	>=15 mins
/wireless-access-point-oper:access-point-oper-data/radio-oper-stats	>=60 secs
/wireless-access-point-oper:access-point-oper-data/radio-oper-data	>=180 secs
/wireless-access-point-oper:access-point-oper-data/oper-data	>=180 secs
/wireless-rrm-oper:rrm-oper-data/rrm-measurement	>=180 secs
/wireless-client-oper:client-oper-data/dot11-oper-data	>=180 secs
/wireless-client-oper:client-oper-data/common-oper-data	>=15 mins
/wireless-client-oper:client-oper-data/policy-data	>=60 secs
/wireless-client-oper:client-oper-data/sisf-db-mac/ipv4-binding/ip-key/ip-addr	>=15 mins
/wireless-client-oper:client-oper-data/traffic-stats	>=180 secs
/lldp-ios-xe-oper:lldp-entries/lldp-state-details	>=60 secs
/device-hardware-xe-oper:device-hardware-data/device-hardware	>=15 mins
/wireless-mobility-oper:mobility-oper-data/mobility-node-data/ulink-status	>=60 secs
/process-cpu-ios-xe-oper:cpu-usage/cpu-utilization/one-minute	>=60 secs
/platform-sw-ios-xe-oper:cisco-platform-software/control-processes	>=60 secs
/environment-ios-xe-oper:environment-sensors/environment-sensor	>=60 secs
/lldp-ios-xe-oper:lldp-entries/lldp-intf-details	>=60 secs
/interfaces-ios-xe-oper:interfaces/interface	>=60 secs
/platform-ios-xe-oper:components/component	>=60 secs
/mdt-oper-v2:mdt-oper-v2-data	>=60 secs
/wireless-access-point-oper:access-point-oper-data/radio-oper-data/radio-band-info	>=180 secs

Subscription

A subscription binds one or more Gather points and destinations. A Multicast Default (MDT) streams data for each Gather point at the configured frequency (cadence-based streaming).

Transport

The protocol that is used for the connection between a publisher and a receiver is known as the transport protocol, and this decides how data are transmitted. This protocol is independent of the management protocol for configured subscriptions. The supported transport protocols are gNMI and gRPC. The gNMI transport protocol supports JSON encoding of data, while gRPC supports Key-value Google Protocol Buffers (kvGPB) encoding.

Scale Considerations

The following table provides the scale numbers that are applicable to the native model for an XPath set.

Table 62: Scaling Considerations to the Native Model

Attribute	Scale
AP	4000
Client	15000
SSID Per AP	6
BSSID per AP	12
Neighbors per AP	60 (30x2)
Number of Physical Neighbor APs	49
Number of Neighbor Records	60000 records

Session

You can choose to initiate the subscription by establishing a telemetry session between the controller and the receiver. A telemetry session can be initiated using:

- gNMI Dial-In Mode
- gRPC Dial-Out Mode

gNMI Dial-In-Mode

In a dial-in mode, a Model-Driven Telemetry (MDT) receiver dials in to the controller, and subscribes dynamically to one or more Gather points or subscriptions. The controller acts as the server, and the receiver as the client. The controller streams telemetry data through the same session. The dial-in mode of subscriptions is dynamic, which gets terminated when the receiver cancels the subscription or when the session is terminated.

gRPC- Dial-Out-Mode

In a dial-out mode, the controller dials out to the receiver. Here the controller acts as a client and receiver acts as a server. In this mode, Gather points and destinations are configured and bound together into one or more subscriptions. The controller continually attempts to establish a session with each destination in the subscription, and streams data to the receiver. The dial-out mode of subscriptions is persistent.

Figure 23: Telemetry Session

The following figure explains the telemetry session:



Configuring Telemetry on a Cisco Catalyst 9800 Series Wireless Controller

To configure telemetry on a Cisco Catalyst 9800 Series Wireless Controller, perform the following:

1. Enable gNXI in an Insecure Mode
2. Enable gNXI in a Secure Mode
3. Verify the Status of the Subscription
4. Manage Configured Subscriptions

Enabling gNXI in Insecure Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode

	Command or Action	Purpose
	Example: `Device# enable`	Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**gnxi** **Example:** `Device(config)# gnxi`	Starts the gNXI process.
Step 4	**gnxi server** **Example:** `Device(config)# gnxi server`	Enables the gNXI server in insecure mode.
Step 5	**gnxi port** *port-number* **Example:** `Device(config)# gnxi 50000`	Sets the gNXI port. The default insecure gNXI port is 9339.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 7	**show gnxi state** **Example:** `Device# show gnxi state`	Displays the status of gNXI server.

Example

The following is a sample output of the **show gnxi state** command:

```
Device# show gnxi state
State Status
--------------------------------
Enabled Up
```

Enabling gNXI in Secure Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**gnxi** **Example:** `Device(config)# gnxi`	Starts the gNXI process.
Step 4	**gnxi secure-server** **Example:** `Device(config)# gnxi secure-server`	Enables the gNXI server in secure mode.
Step 5	**gnxi secure-trustpoint** *trustpoint-name* **Example:** `Device(config)# gnxi secure-trustpoint`	Specifies the trustpoint and certificate set that gNXI uses for authentication.
Step 6	**gnxi secure-client-auth** **Example:** `Device(config)# gnxi secure-client-auth`	(Optional) The gNXI process authenticates the client certificate against the root certificate.
Step 7	**gnxi secure-port** **Example:** `Device(config)# gnxi secure-port`	(Optional) Sets the gNXI port. • The default insecure gNXI port is 9339.
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 9	**show gnxi state** **Example:** `Device# show gnxi state`	Displays the gNXI servers status.

Example

The following is sample output from the **show gnxi state** command:

```
Device# show gnxi state
State Status
--------------------------------
Enabled Up
```

Verifying the Status of a Telemetry Subscription on a Cisco Catalyst 9800 Series Wireless Controller

To verify the status of a subscription, use the following command:

```
Device# show telemetry ietf subscription all
Device# show telemetry ietf subscription 101
Device# show telemetry ietf subscription 101 detail
Device# show telemetry ietf subscription 101 receiver
Device# show telemetry internal connection
Device# show telemetry internal subscription all stats
Device# show telemetry receiver all
Device# show telemetry receiver name <receivers-name>
Device# show telemetry connection all
```

Managing Configured Subscriptions on a Cisco Catalyst 9800 Series Wireless Controller

Use the **show platform software ndbman switch** {*switch-number* | **active**| **standby**} **models** command to display the list of YANG models that support on-change subscription.

Note Currently, you can only use the gRPC protocol for managing configured subscriptions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**telemetry ietf subscription** *id* **Example:** `Device(config)# telemetry ietf subscription 112`	Creates a telemetry subscription and enters telemetry-subscription mode.
Step 4	**encoding encode-kvgpb** **Example:** `Device(config-mdt-subs)# encoding encode-kvgpb`	Specifies the Key-value Google Protocol Buffers (kvGPB) encoding.

	Command or Action	Purpose
Step 5	**filter xpath** *path* **Example:** `Device(config-mdt-subs)# filter xpath /wireless-access-point-oper:access-point-oper-data/capwap-data`	Specifies the XPath filter for the subscription.
Step 6	**source-address**{ *A.B.C.D* | *X:X:X:X::X* } **Example:** `Device(config-mdt-subs)# source-address ip-address 209.165.200.225 | 2001:DB8::1`	Configures the source IP address on the telemetry subscription interface.
Step 7	**stream yang-push** *path* **Example:** `Device(config-mdt-subs)# stream yang-push`	Configures a stream for the subscription.
Step 8	**update-policy {on-change | periodic}** *period* **Example:** `Device(config-mdt-subs)# update-policy periodic 3000`	Configures a periodic update policy for the subscription.
Step 9	**receiver ip address** *ip-address receiver-port* **protocol** *protocol* **profile** *name* **Example:** `Device(config-mdt-subs)# receiver ip address 209.165.201.1 protocol grpc-tcp`	Configures a periodic update policy for the subscription.
Step 10	**end** **Example:** `Device(config-mdt-subs)# end`	Exits telemetry-subscription configuration mode and returns to privileged EXEC mode.

Zero Trust Telemetry

To configure zero trust telemetry on a Cisco Catalyst 9800 Series Wireless Controller, perform the following:

1. Define a protocol
2. Define a named receiver
3. Configure telemetry subscription

Define a Protocol

Before you begin

Define crypto trustpoints (CAforMDTserver and IDforWLCclient) and certificates before the telemetry configuration.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**telemetry protocol grpc profile** *profile-name* **Example:** `Device(config)# telemetry protocol grpc profile mtlsyang`	Configures the protocol gRPC profile and enters gRPC profile name.
Step 3	**ca-trustpoint** *ca-for-mdt-server* **Example:** `Device(config-mdt-protocol-grpc-profile)# ca-trustpoint CAforMDTserver`	Adds the server CA trustpoint.
Step 4	**id-trustpoint** *wlc-id-trustpoint* **Example:** `Device(config-mdt-protocol-grpc-profile)# id-trustpoint IDforWLCclient`	Adds the client ID trustpoint.

Define a Named Receiver

This procedure defines:

- FQDN DNS name
- Crypto protocol definition

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**telemetry receiver protocol** *receiver-name* **Example:** `Device(config)# telemetry receiver protocol collector`	Configures the receiver name.

	Command or Action	Purpose
Step 3	**host name** *FQDN-receiver* **Example:** `Device(config-mdt-protocol-receiver)# host name collector-telemetry.cisco.com 57500`	Adds FQDN DNS name of receiver.
Step 4	**protocol grpc-tls profile** *profile-name* **Example:** `Device(config-mdt-protocol-receiver)# protocol grpc-tls profile mtlsyang`	Defines the gRPC TLS profile named mtlsyang.

Configure Telemetry Subscription

This procedure configures:

- Xpath
- Named receiver
- Protocol

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**telemetry ietf subscription** *id* **Example:** `Device(config)# telemetry ietf subscription 113`	Creates a telemetry subscription and enters telemetry-subscription mode.
Step 4	**encoding encode-kvgpb** **Example:** `Device(config-mdt-subs)# encoding encode-kvgpb`	Specifies the Key-value Google Protocol Buffers (kvGPB) encoding.
Step 5	**filter xpath** *path* **Example:** `Device(config-mdt-subs)# filter xpath /wireless-ble-ltx-oper:ble-ltx-oper-data/ble-ltx-ap-streaming`	Specifies the XPath filter for the subscription.

	Command or Action	Purpose
Step 6	**source-address** { *A.B.C.D* | *X:X:X:X::X* } **Example:** `Device(config-mdt-subs)# source-address ip-address 209.165.200.225 | 2001:DB8::1`	Configures the source IP address on the telemetry subscription interface.
Step 7	**stream yang-push** **Example:** `Device(config-mdt-subs)# stream yang-push`	Configures a stream for the subscription.
Step 8	**update-policy {on-change | periodic}** *period* **Example:** `Device(config-mdt-subs)# update-policy periodic 6000`	Configures a periodic update policy for the subscription.
Step 9	**receiver-type protocol** **Example:** `Device(config-mdt-subs)# receiver-type protocol`	Configures type protocol for receiver.
Step 10	**receiver name** *receiver-name* **Example:** `Device(config-mdt-subs)# receiver name collector`	Specifies the receiver name.
Step 11	**end** **Example:** `Device(config-mdt-subs)# end`	Exits telemetry-subscription configuration mode and returns to privileged EXEC mode.

On-Change Telemetry Support

From Cisco IOS XE Cupertino 17.7.1 onwards, on-change telemetry support is provided to a subset of XPaths.

Supported XPaths for On-Change Subscription

The following table lists the supported XPaths for on-change subscription.

Table 63: Supported Gather Points and XPaths

Gather Points	XPaths
/access-point-oper-data/radio-operdata/	/access-point-oper-data/radio-operdata/ phy-ht-cfg/cfg-data/curr-freq

Gather Points	XPaths
	/access-point-oper-data/radio-operdata/phy-ht-cfg/cfg-data/chan-width
	/access-point-oper-data/radio-oper-data/current-band-id
/access-point-oper-data/capwap-data	/access-point-oper-data/capwap-data/name
	/access-point-oper-data/capwapdata/device-detail/wtp-version/sw-ver/version
	/access-point-oper-data/capwap-data/device-detail/wtp-version/sw-ver/release
	/access-point-oper-data/capwapdata/device-detail/wtp-version/sw-ver/maint
	/access-point-oper-data/capwapdata/device-detail/wtp-version/sw-ver/build
	/access-point-oper-data/capwap-data/ap-state/ap-operation-state
	/access-point-oper-data/capwapdata/device-detail/static-info/board-data/wtp-serial-num
/access-point-oper-data/oper-data	/access-point-oper-data/oper-data/ap-ip-data/ap-ip-addr
	/access-point-oper-dat/oper-data/ap-pow/power-type

The following table lists the XPaths that are introduced in Cisco-IOS-XE-wireless-ap-global-oper-transform.yang model that is displayed through telemetry feed.

Table 64: Supported Gather Points and XPaths (Cisco-IOS-XE-wireless-ap-global-oper-transform.yang)

Gather Points	XPaths
/ap-global-oper-data/ap-join-stats/wtp-mac	/ap-global-oper-data/ap-join-stats/ap-join-info/ap-ethernet-mac
	/ap-global-oper-data/ap-join-stats/ap-join-info/ap-name
	/ap-global-oper-data/ap-join-stats/ap-join-info/ap-ip-addr
	/ap-global-oper-data/ap-join-stats/ap-join-info/is-joined
	/ap-global-oper-data/ap-join-stats/ap-join-info/last-error-type
	/ap-global-oper-data/ap-join-stats/ap-disconnect-reason

The following table lists the XPaths that are introduced in Cisco-IOS-XE-aaa-oper.yang model to support aaa/radius/radsec and displayed through telemetry feed.

Table 65: Supported Gather Points and XPaths (Cisco-IOS-XE-aaa-oper.yang)

Gather Points	Xpaths
/aaa-data/aaa-radius-stats/	/aaa-data/aaa-radius-stats/radsec-pkt-cnt-idletime
	/aaa-data/aaa-radius-stats/radsec-send-hs-start-cnt
	/aaa-data/aaa-radius-stats/radsec-hs-success-cnt
	/aaa-data/aaa-radius-stats/radsec-total-tx-pkt-cnt
	/aaa-data/aaa-radius-stats/radsec-total-rx-pkt-cnt
	/aaa-data/aaa-radius-stats/radsec-total-conn-rst-cnt
	/aaa-data/aaa-radius-stats/radsec-conn-rst-cnt-idle /aaa-data/aaa-radius-stats/radsec-conn-rst-cnt-noresp
	/aaa-data/aaa-radius-stats/radsec-conn-rst-cnt-malpkt
	/aaa-data/aaa-radius-stats/radsec-conn-rst-cnt-err
	/aaa-data/aaa-radius-stats/radsec-conn-rst-cnt-peer
	/aaa-data/aaa-radius-stats/num-aaa-lib-inst
	/aaa-data/aaa-radius-stats/server-detail
/aaa-data/aaa-radius-global-stats	/aaa-data/aaa-radius-global-stats/access-rejects
	/aaa-data/aaa-radius-global-stats/access-accepts
	/aaa-data/aaa-radius-global-stats/authen-responses-seen
	/aaa-data/aaa-radius-global-stats/authen-with-response
	/aaa-data/aaa-radius-global-stats/authen-without-response
	/aaa-data/aaa-radius-global-stats/authen-avg-response-delay
	/aaa-data/aaa-radius-global-stats/authen-max-response-delay
	/aaa-data/aaa-radius-global-stats/authen-timeouts
	/aaa-data/aaa-radius-global-stats/authen-duplicate-id
	/aaa-data/aaa-radius-global-stats/authen-bad-authenticators
	/aaa-data/aaa-radius-global-stats/acct-responses-seen
	/aaa-data/aaa-radius-global-stats/acct-with-response

Gather Points	Xpaths
	/aaa-data/aaa-radius-global-stats/acct-without-response
	/aaa-data/aaa-radius-global-stats/acct-avg-response-delay
	/aaa-data/aaa-radius-global-stats/acct-max-response-delay
	/aaa-data/aaa-radius-global-stats/acct-timeouts
	/aaa-data/aaa-radius-global-stats/acct-duplicate-id
	/aaa-data/aaa-radius-global-stats/acct-bad-authenticators
	/aaa-data/aaa-radius-global-stats/stats-time

The following table lists the XPaths that are introduced in Cisco-IOS-XE-wireless-mesh-rpc.yang model to support the mesh-related EXEC commands:

Table 66: Supported EXEC CLIs and XPaths (Cisco-IOS-XE-wireless-mesh-rpc.yang)

EXEC CLI	XPath
ap name <*ap-name*> [no] mesh ethernet [0|1|2|3] mode trunk vlan allowed <*vlan-id*>	/set-rad-mesh-ethernet-trunk-allowed-vlan
ap name <*ap-name*> [no] mesh ethernet [0|1|2|3] mode trunk vlan native	/set-rad-mesh-ethernet-trunk-native-vlan
ap name <*ap-name*> mesh linktest <*dst AP MAC*> <*data rate*> <*packets/sec*> <*packet size*> <*duration*>	/exec-linktest-ap
ap name <*ap-name*> [no] mesh ethernet [0|1|2|3] mode access <*vlan-id*>	/set-rad-mesh-ethernet-access-vlan
ap name <*ap-name*> [no] mesh block-child	/set-rad-mesh-block-child
ap name <*ap-name*> [no] mesh vlan-trunking	/set-rad-mesh-trunking
ap name <*ap-name*> [no] mesh daisy-chaining strict-rap	/set-rad-mesh-daisy-chain-strict-rap
ap name <*ap-name*> [no] mesh daisy-chaining	/set-rad-mesh-daisy-chain-mode
ap name <*ap-name*> [no] mesh parent preferred	/set-rad-mesh-preferred-parent-ap
ap name <*ap-name*> mesh backhaul rate dot11ac mcs <*mcs-index*> *ss* <*1-4*>	/set-rad-mesh-bhaul-tx-rate
ap name <*ap-name*> mesh backhaul radio dot11 5ghz [slot <*slot-id*>]	/set-rad-mesh-bhaul-radio
ap name <*ap-name*> mesh security psk provisioning delete	/set-rad-mesh-security-psk-provisioning-delete

EXEC CLI	XPath
ap name <*ap-name*> mesh vlan-trunking native <*vlan-id*>	/set-rad-mesh-trunking-vlan

The following table lists the XPaths that are introduced in Cisco-IOS-XE-aaa-oper.yang model to support radius EXEC commands:

Table 67: Supported EXEC CLIs and XPaths (Cisco-IOS-XE-aaa-oper.yang)

EXEC CLIs	XPaths
show radius statistic	/aaa-data/aaa-radius-global-stats/

Troubleshooting Telemetry Support

This document outlines a set of commands for gathering data from Cisco Catalyst 9800 Series Wireless Controller, specifically focused on addressing gRPC telemetry-related issues in support of TAC cases.

Here are a few factors to consider when conducting troubleshooting steps:

- Provide a clear problem description.
- What has changed in the network?
- What was the previous working day/time?
- What is the impact of this problem?

Note Run all the **show** commands with **show clock** or **terminal exec prompt timestamp** once to log timestamps automatically.

General Guidelines

For every issue, run the following commands:

1. `Device# terminal length 0`
2. `Device# show clock`
3. `Device# show tech-support wireless`
4. `Device# request platform software trace archive last 1`

Perform Basic Checks

1. Verify that the requisite processes (particularly pubd) are running using the following commands:

   ```
   show platform software yang-management process
   ```

2. Capture and validate the telemetry-specific configuration using the following command:

```
show running-config | section telemetry
```

3. Check the validity of any subscriptions using the following command:

```
show telemetry ietf subscription all
```

4. Check the validity of any named receivers using the following command:

```
show telemetry receiver all
```

5. Verify the telemetry subscription states using the following command:

```
show telemetry internal subscription all stats
```

Check Connectivity Issues

1. Check the state of the subscription receiver using the following commands:

```
show telemetry ietf subscription <id> receiver
```

2. Check the state of telemetry connections using the following command:

```
show telemetry connection all
```

3. Check which subscriptions use a particular connection using the following command:

```
show telemetry connection <index> subscription
```

Capture Debug Logs

1. Enable the following debug options:

```
set platform software trace mdt-pubd chassis active r0 mdt-ctrl debug
set platform software trace mdt-pubd chassis active r0 pubd debug
set platform software trace mdt-pubd chassis active r0 green-be debug
set platform software trace mdt-pubd chassis active r0 green-fe debug
set platform software trace mdt-pubd chassis active r0 dbal debug
set platform software trace mdt-pubd chassis active r0 tdllib debug
set platform software trace ios chassis active r0 green-be debug
set platform software trace ios chassis active r0 dbal debug
set platform software trace ios chassis active r0 tdllib debug
```

2. Recreate the problem.

3. Collect debug logs:

```
request platform software trace archive last <days>
```

4. Disable debugging using the following commands:

```
set platform software trace mdt-pubd chassis active r0 mdt-ctrl notice
set platform software trace mdt-pubd chassis active r0 pubd notice
set platform software trace mdt-pubd chassis active r0 green-be notice
set platform software trace mdt-pubd chassis active r0 green-fe notice
set platform software trace mdt-pubd chassis active r0 dbal notice
set platform software trace mdt-pubd chassis active r0 tdllib notice
set platform software trace ios chassis active r0 green-be notice
set platform software trace ios chassis active r0 dbal notice
set platform software trace ios chassis active r0 tdllib notice
```

General Telemetry Diagnostics

To capture general telemetry diagnostics, use the following command:

```
show telemetry internal diagnostics
```

Generate a Core

Generate a core using the following commands:

1. `show clock`
2. `configure terminal`
3. `service internal`
4. `end`
5. `request platform software process core mdt-pubd chassis active r0`

Disable Logging

Disable the logging using the following commands:

1. `configure terminal`
2. `no service internal`
3. `end`

Capture CPU Memory

To capture CPU memory details use the following commands:

- `show processes cpu platform sorted | i pubd`
- `show processes memory platform sorted | s pubd`

Cisco Catalyst Center Client Event and SSID Telemetry Filter

Feature History for Cisco Catalyst Center Client Event and SSID Telemetry Filter

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 68: Feature History for Cisco Catalyst Center Client Event and SSID Telemetry Filter

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Cisco Catalyst Center Client Event and SSID Telemetry Filter	This feature filters out telemetry data for a configured SSID on the controller and AP.

Information About Cisco Catalyst Center Client Event and SSID Telemetry Filter

Locations such as airports, shopping malls, and so on have wireless guest networks with thousands of transient guest clients. The transient guest clients mix the telemetry data and its subsequent health scores with clients that require assurance (for instance, in a corporate WLAN). This poses a scaling challenge as Cisco Catalyst Center tries to keep up with the receiving high-frequency telemetry data and maintaining history of the transient clients.

This feature addresses the requirement by filtering out the telemetry data for a configured SSID on the controller and AP.

Figure 24: High-Level End-to-End System Flow for Cisco Catalyst Center Client Event and SSID Telemetry Filter



Cisco Catalyst Center configures the Complex Event Processing (CEP) transform with the SSID for which the telemetry data needs to be filtered out along with the subscriptions. The Publishing Daemon (PubD) module in the controller filters out the data based on the configured transform.

Note The Cisco Catalyst Center automation takes care of pushing the transforms. You must enable or disable filtering for a specific SSID in the controller GUI.

To debug the filtering done at PubD, run the following commands in the controller:

```
Device# set platform software trace mdt-pubd chassis active r0 pubd debug
set platform software trace mdt-pubd chassis active r0 mdt-xfrm debug
```

Cisco Catalyst Center configures WLAN for which iCAP data needs to be filtered in an AP profile. The controller then pushes the configuration to the corresponding APs. The AP then programs the **aptrace** module to drop the packets and events for the filtered SSID. The filtered data covers the following:

- Client events
- Client statistics
- AP or RF statistics
- Partial PCAP
- Anomaly detection

Restrictions for Cisco Catalyst Center Client Event and SSID Telemetry Filter

- CLI configuration is applicable for WLAN and not SSID. The Cisco Catalyst Center automation covers one-to-one mapping of WLAN to SSID.
- Controller does not send any notification to Cisco Catalyst Center at the beginning or at the end of filtering.
- Controller GUI configuration is not supported.

Supported Workflow for Cisco Catalyst Center Client Event and SSID Telemetry Filter

- Creating WLANs.
- Mapping WLAN to a Policy Profile.
- Creating a filter for WLAN in AP Join Profile.

Enabling iCAP Filtering in APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**description** *ap-profile-name* **Example:** `Device(config-ap-profile)# description "xyz ap profile"`	Adds a description for the AP profile.
Step 4	**icap subscription client exclude telemetry-data wlan** *wlan-profile-name* **Example:** `Device(config-ap-profile)# icap subscription client exclude telemetry-data wlan wlan-name`	Enables iCAP filtering in APs.

Disabling Client Telemetry Data for a WLAN (YANG)

To disable the client telemetry data for a WLAN, use the following RPC model:

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:0a77124f-c563-469d-bd21-cc625a9691cc">
<nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<site-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-site-cfg">
<ap-cfg-profiles>
<ap-cfg-profile>
<profile-name nc:operation="merge">default-ap-profile</profile-name>
<icap-client-exclude-cfgs>
<icap-cient-exclude-cfg nc:operation="merge">
<wlan-profile nc:operation="merge">tel</wlan-profile>
</icap-client-exclude-cfg>
</cap-client-exclude-cfgs>
</ap-cfg-profile>
</ap-cfg-profiles>
</site-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>
```

For more information on YANG models, see the *Cisco IOS XE Programmability Configuration Guide* and YANG Data Models on Github at https://github.com/YangModels/yang/tree/master/vendor/cisco/xe.

You can contact the Developer Support Community for NETCONF/YANG features using the following link:

https://developer.cisco.com/

Verifying Client Telemetry Data for a WLAN

To verify the client telemetry data for a WLAN, use the following command:

```
Device# show running-config | section profile
ap profile default-ap-profile
 capwap retransmit count 8
 capwap timers primary-discovery-timeout 3000
 country IN
 description "default ap profile"
 icap subscription client exclude telemetry-data wlan guest
```



CHAPTER 86

Application Performance Monitoring

- Feature History for Application Performance Monitoring, on page 915
- Information About Application Performance Monitoring, on page 915
- Restrictions for Application Performance Monitoring, on page 916
- Workflow, on page 916
- Verify Application Performance Monitoring, on page 920

Feature History for Application Performance Monitoring

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 69: Feature History for Application Performance Monitoring

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Application Performance Monitoring	This feature collects and exports assurance-related metrics (per application) of the flows forwarded through AP to the Cisco DNA Centre Assurance application.

Information About Application Performance Monitoring

Application Performance Monitoring feature collects and exports assurance-related metrics (per application) of the flows that are forwarded through specific interfaces of the access point to the Cisco Catalyst Center Assurance application. This feature supports two monitors—a general assurance monitor that computes quantitative metrics for TCP and UDP flows and qualitative metrics for TCP flows and a media monitor that computes qualitative and quantitative metrics for real-time protocol (RTP) flows. Voice applications such as Microsoft Teams and Session Initiation Protocol (SIP) use RTP monitors, while other applications use TCP and UDP monitor.

A flow monitor can be attached to:

- A interface that monitors all the flows from the attachment point.

- A wireless profile policy (the wireless profile policy that is associated with a WLAN or SSID) that monitors all the traffic passing through it.

Assurance performance monitoring is supported on the following platforms:

- Cisco Catalyst 9800 Series Controllers (9800-80, 9800-40, 9800-L, and 9800-CL)
- Cisco Catalyst 9100 Series APs (FlexConnect and fabric mode)
- Cisco Catalyst 9300 Series and 9400 Series switches (fabric mode)

Restrictions for Application Performance Monitoring

- Local flow exporter is not supported.
- The following commands are not supported:
  - **show avc wlan application top**
  - **show avc client top application**
- You cannot configure Application Performance Monitoring and Application Visibility and Control basic on a single policy profile. You can configure them only on two separate policy profiles.
- During CAPWAP restart, AP moves to standby mode, and the nitro engine is disabled. When CAPWAP is up and the nitro engine is enabled, an attempt is made to classify the flows. Since there is not enough information to classify the applications, they are marked as unknown. When the AP rejoins CAPWAP, client traffic gets marked or classified correctly.
- When a client roams while an application has an active-session, the specific session traffic is marked as unknown. The client has to start a new session to mark or classify the traffic correctly.

Workflow

Create a Flow Monitor

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor avc_assurance`	Creates a flow monitor.

	Command or Action	Purpose
Step 3	**description** *description* **Example:** `Device(config-flow-monitor)# description assurance monitor ID is 90`	Adds a description to the flow monitor.
Step 4	**record wireless avc** {**ipv4** | **ipv6**} **assurance** **Example:** `Device(config-flow-monitor)# record wireless avc ipv4 assurance`	Specifies the IPv4 assurance metrics for wireless.
Step 5	**exit** **Example:** `Device(config-flow-monitor)# exit`	Returns to global configuration mode.
Step 6	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor avc_assurance_rtp`	Creates a flow monitor.
Step 7	**description** *description* **Example:** `Device(config-flow-monitor)# description assurance-rtp monitor ID is 94`	Adds a description to the flow monitor.
Step 8	**record wireless avc** {**ipv4** | **ipv6**} **assurance-rtp** **Example:** `Device(config-flow-monitor)# record wireless avc ipv4 assurance-rtp`	Specifies the IPv4 assurance RTP metrics for wireless.
Step 9	**end** **Example:** `Device(config-flow-monitor)# end`	Returns to privileged EXEC mode.

Create a Wireless WLAN Profile Policy

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy AVC_POL`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the policy profile.
Step 4	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Disables central switching.
Step 5	**ipv4 flow monitor** *monitor-name* **input** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor avc_assurance input`	Specifies the name of the IPv4 ingress flow monitor.
Step 6	**ipv4 flow monitor** *monitor-name* **input** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor avc_assurance_rtp input`	Specifies the name of the IPv4 ingress flow monitor.
Step 7	**ipv4 flow monitor** *monitor-name* **output** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor avc_assurance output`	Specifies the name of the IPv4 egress flow monitor.
Step 8	**ipv4 flow monitor** *monitor-name* **output** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor avc_assurance_rtp output`	Specifies the name of the IPv4 egress flow monitor.
Step 9	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.
Step 10	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Create a Policy Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy mywlan_ssid`	Configures a policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-avc* **policy** *policy* **Example:** `Device(config-policy-tag)# wlan mywlan_ssid policy AVC_POL`	Attaches the policy tag to a WLAN.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode.

Attach the Policy Profile to an AP

Procedure

	Command or Action	Purpose
Step 1	**ap** *ap-ether-mac* **Example:** `Device(config)# ap 9412.1212.1201`	Enters AP configuration mode.
Step 2	**policy-tag** *policy-tag* **Example:** `Device(config-ap-tag)# policy-tag mywlan_ssid`	Specifies the policy tag that is to be attached to the AP.
Step 3	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode.

Verify Application Performance Monitoring

Use the following commands to verify application performance monitoring configuration.

To check application performance monitoring statistics, use the following commands:

```
Device# show flow exporter statistics

Flow Exporter apm_exp:
  Packet send statistics (last cleared 4w1d ago):
    Successfully sent:         2082                  (216624 bytes)
!Packet sent count sent from controller to Cisco Cisco Catalyst Center
    Reason not given:          1099                  (114296 bytes)

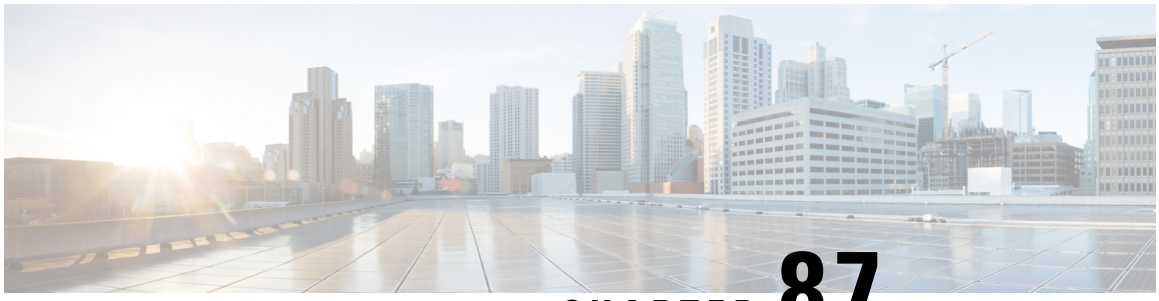
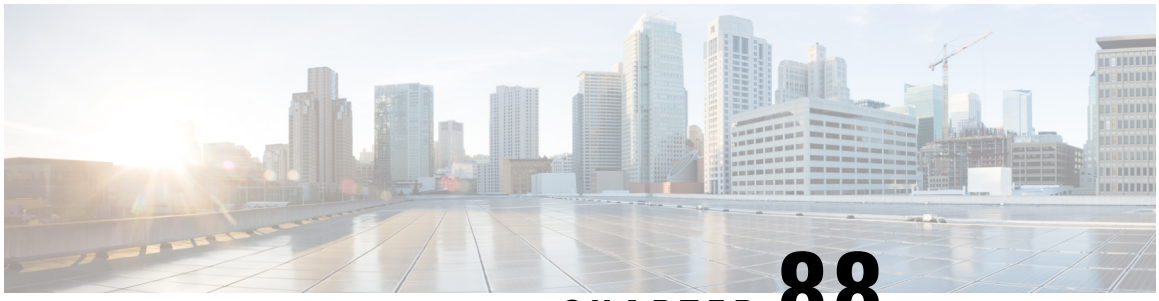
  Client send statistics:
    Client: Flow Monitor avc
      Records added:           0
      Bytes added:             0


Device# show flow monitor assurance cache

Cache type:                                Normal (Platform cache)
  Cache size:                                200000
  Current entries:                                0
  High Watermark:                                 1
!Controller flow monitor cache statistics

  Flows added:                                    6
  Flows aged:                                     6
    - Active timeout      (    10 secs)           6
```

To check status of application performance monitoring, use the following command

```
Device# show avc status

VAP FNF-STATUS AVC-QOS-STATUS SD AVC-STATUS APM-STATUS
!APM-STATUS contains IPv4, IPv6 assurance and assurance-rtp monitors.

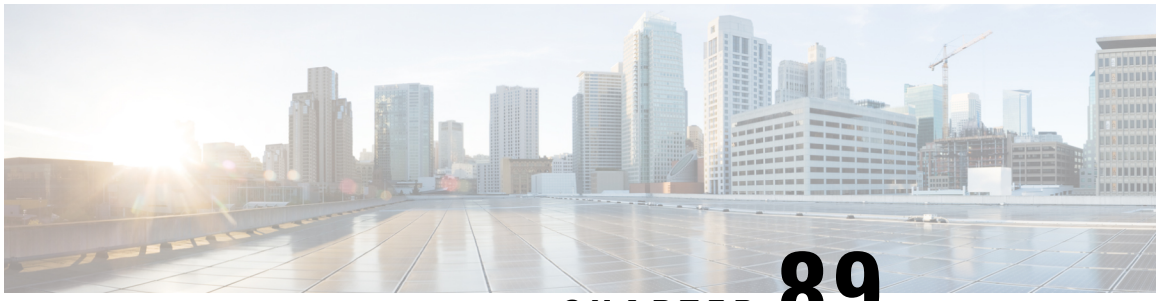
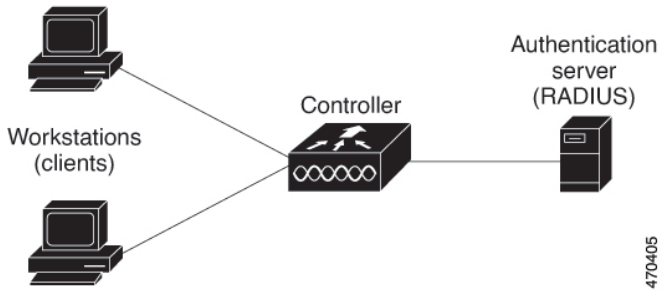
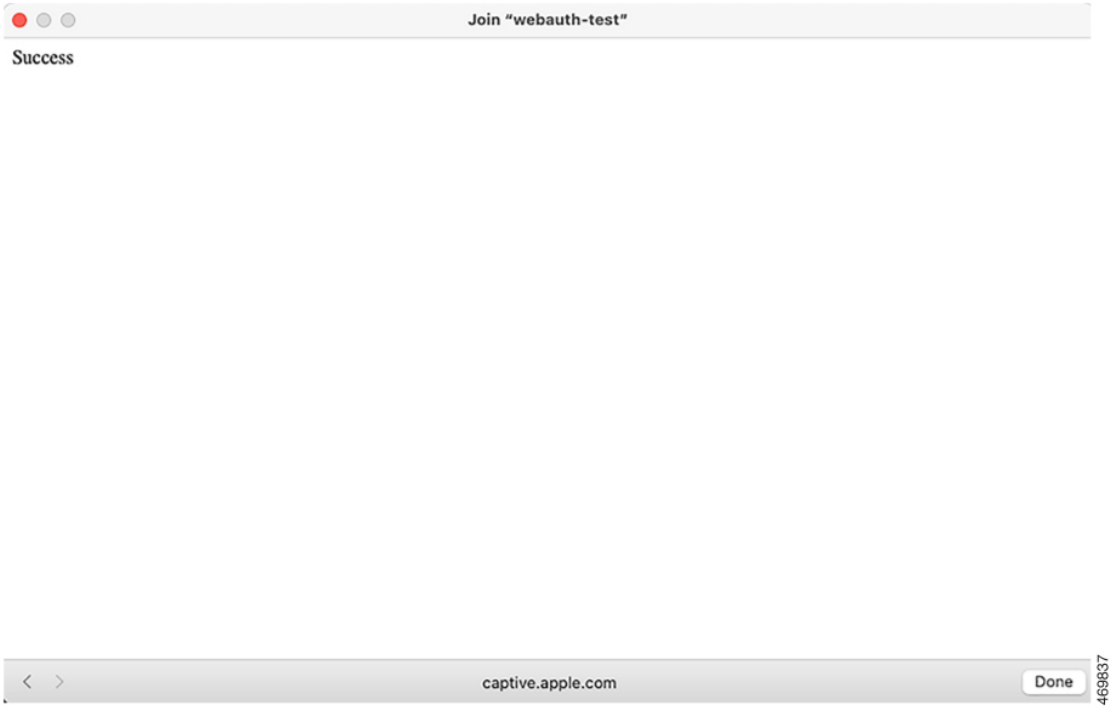
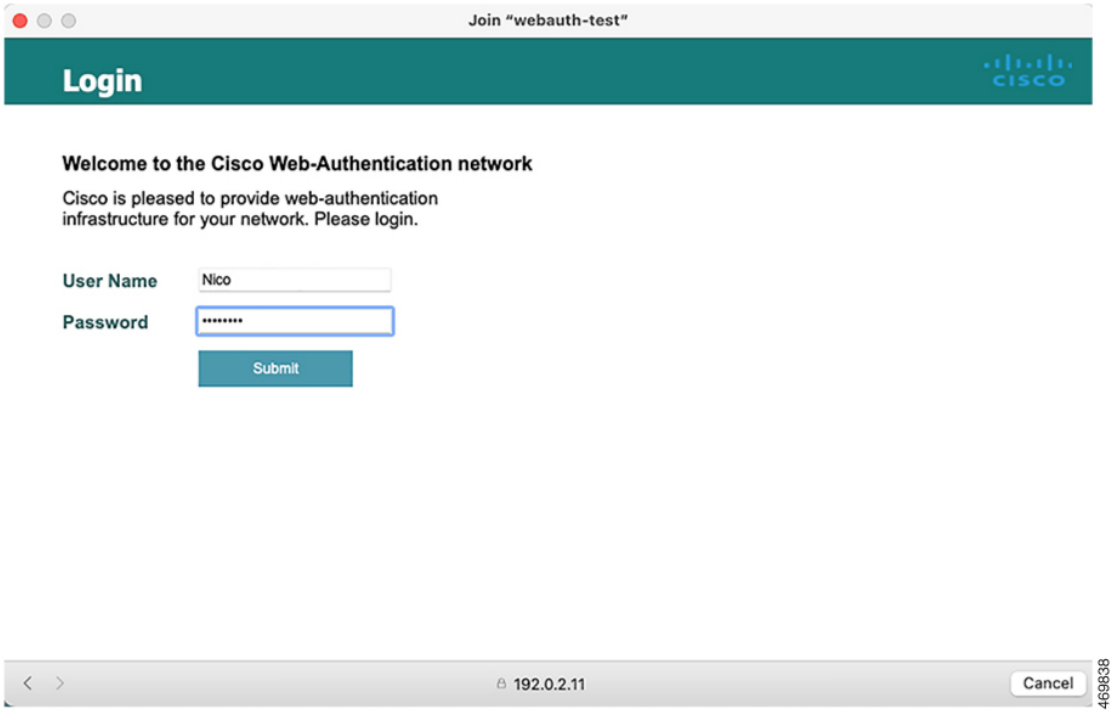
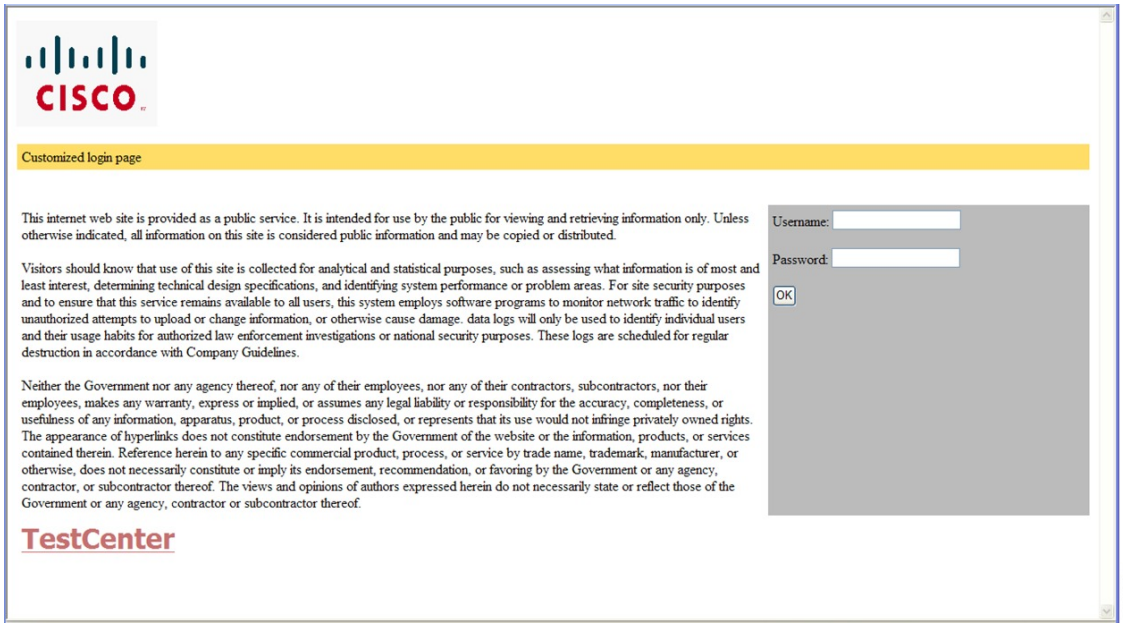
0   Disabled   Disabled       Enabled       IPV4,IPV4-RTP,IPV6,IPV6-RTP
1   Disabled   Disabled       Disabled      Disabled
2   Disabled   Disabled       Disabled      Disabled
3   Disabled   Disabled       Disabled      Disabled
4   Disabled   Disabled       Disabled      Disabled
5   Disabled   Disabled       Disabled      Disabled
6   Disabled   Disabled       Disabled      Disabled
7   Disabled   Disabled       Disabled      Disabled
8   Disabled   Disabled       Disabled      Disabled
9   Disabled   Disabled       Disabled      Disabled
10  Disabled   Disabled       Disabled      Disabled
11  Disabled   Disabled       Disabled      Disabled
12  Disabled   Disabled       Disabled      Disabled
13  Disabled   Disabled       Disabled      Disabled
14  Disabled   Disabled       Disabled      Disabled
15  Disabled   Disabled       Disabled      Disabled
```



CHAPTER 87

Wireless Clients Threshold Warning

- Information About Wireless Clients Threshold Warning, on page 921
- Configuring a Warning Period, on page 921
- Configuring Client Threshold, on page 922

Information About Wireless Clients Threshold Warning

Cisco IOS XE Bengaluru 17.6.x introduces the Wireless Clients Threshold Warning feature, which allows you to configure a warning message when the number of simultaneous wireless clients on the controller breaches a set threshold. By default, the threshold is set to 75 percent of the total capacity. For example, Cisco Catalyst 9800-80 Wireless Controller supports up to 64,000 clients, and the threshold is set at 48,000 client. When the threshold is breached, the controller sends notifications to the corresponding user using syslog messages, SNMP traps, and NETCONF/Yang notifications.

The Wireless Clients Threshold Warning feature allows you to take note of the impending wireless client limit and act on it before reaching the maximum limit, or modify the number of wireless clients allowed on a controller, as required.

The Wireless Clients Threshold Warning feature is enabled by default. To disable the feature, use the **no wireless max-warning** command.

Configuring a Warning Period

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless max-warning period** *interval-in-mins* **Example:** `Device(config)# wireless max-warning period 20`	Configures the periodicity of the wireless client check. Valid values range from 1 to 60 minutes.

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring Client Threshold

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless max-warning threshold clients** *threshold_percentage* **Example:** `Device(config)# wireless max-warning threshold clients 90`	Configures the warning threshold percentage for the maximum number of wireless clients. Valid values range from 50 to 100 percent.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

PART VII

Security

- MAC Filtering, on page 925
- Web-Based Authentication , on page 931
- Central Web Authentication, on page 985
- Private Shared Key, on page 1005
- Multi-Preshared Key, on page 1013
- Multiple Authentications for a Client, on page 1021
- Wi-Fi Protected Access 3, on page 1047
- IP Source Guard, on page 1081
- 802.11w, on page 1083
- Management Frame Protection, on page 1091
- IPv4 ACLs , on page 1095
- Downloadable ACL, on page 1123
- DNS-Based Access Control Lists, on page 1129
- Allowed List of Specific URLs, on page 1147
- Cisco Umbrella WLAN, on page 1151
- RADIUS Server Load Balancing, on page 1163
- AAA Dead-Server Detection, on page 1167
- ISE Simplification and Enhancements, on page 1171
- RADIUS DTLS, on page 1185
- Policy Enforcement and Usage Monitoring, on page 1197
- Local Extensible Authentication Protocol, on page 1201
- Local EAP Ciphersuite, on page 1209
- Authentication and Authorization Between Multiple RADIUS Servers, on page 1213
- CUI Information in RADIUS Accounting, on page 1223

- Secure LDAP, on page 1225
- Network Access Server Identifier, on page 1233
- Locally Significant Certificates, on page 1239
- Certificate Management, on page 1269
- Controller Self-Signed Certificate for Wireless AP Join, on page 1273
- Managing Rogue Devices, on page 1281
- Classifying Rogue Access Points, on page 1301
- Advanced WIPS, on page 1311
- Cisco TrustSec, on page 1321
- SGT Inline Tagging and SXPv4, on page 1335
- Multiple Cipher Support, on page 1341
- Configuring Secure Shell , on page 1345
- Encrypted Traffic Analytics, on page 1353
- FIPS, on page 1367
- Internet Protocol Security, on page 1373
- Transport Layer Security Tunnel Support, on page 1389
- Configuring RFC 5580 Location Attributes, on page 1395
- IP MAC Binding, on page 1407
- Disabling IP Learning in FlexConnect Mode, on page 1409
- Disabling Device Tracking to Support NAC Devices, on page 1411



CHAPTER 88

MAC Filtering

- MAC Filtering, on page 925
- Configuring MAC Filtering for Local Authentication (CLI), on page 927
- Configuring MAC Filtering (GUI), on page 928
- Configuring MAB for External Authentication (CLI), on page 928

MAC Filtering

You can configure the controller to authorize clients based on the client MAC address by using the MAC filtering feature.

When MAC filtering is enabled, the controller uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. The controller sends the authentication server a RADIUS-access/request frame with a username and password based on the client MAC address as soon as it gets the association request from the client. If authorization succeeds, the controller sends a successful association response to the client. If authorization fails, the controller rejects the client association.

Clients that were authorized with MAC filtering can be re-authenticated through the WLAN session timeout feature.

MAC Filtering Configuration Guidelines

- MAC filtering authentication occurs at the 802.11 association phase and delays the association response until authentication is done. If you use a RADIUS server for MAC filtering, it is advised to keep a low latency between the controller and the RADIUS server. When latency is too high, the client might timeout while waiting for the association response.
- MAC filtering can be combined with other authentication methods such as 802.1X, Pre-Shared Key or it can be used alone.
- MAC addresses can be spoofed and MAC filtering does not consist in a security measure.
- Many clients can use a private MAC address to connect and change it at every session, therefore making it harder to identify devices through their MAC address.

Note If wlan-profile-name is configured for a user, guest user authentication is allowed only from that WLAN.

If wlan-profile-name is not configured for a user, guest user authentication is allowed on any WLAN.

The AP fails to join the controller due to an authentication rejection on the RADIUS server. The failure occurs on the Cisco Catalyst 9800 controller, only when the RADIUS server is configured to authenticate the APs with method MAB as endpoints. The reason is that the RADIUS calling-station-id attribute is required for MAB authentication and is not present within the access request packet during the AP join. The workaround is to use a different AP authentication method than MAB as endpoints such as PAP-ASCII using a username and a password.

If you want the client to connect to SSID1, but not to SSID2 using mac-filtering, ensure that you configure **aaa-override** in the policy profile.

In the following example, when a client with MAC address 1122.3344.0001 tries to connect to a WLAN, the request is sent to the local RADIUS server, which checks the presence of the client MAC address in its attribute list (FILTER_1 and FILTER_2). If the client MAC address is listed in an attribute list (FILTER_1), the client is allowed to join the WLAN (WLAN_1) that is returned as *ssid attribute* from the RADIUS server. The client is rejected, if the client MAC address is not listed in the attribute list.

Local RADIUS Server Configuration

```
!Configures an attribute list as FILTER_2
aaa attribute list FILTER_2
!Defines an attribute type that is to be added to an attribute list.
attribute type ssid "WLAN_2"

!Username with the MAC address is added to the filter
username 1122.3344.0001 mac aaa attribute list FILTER_2

!
aaa attribute list FILTER_1
attribute type ssid "WLAN_1"
username 112233440001 aaa attribute list FILTER_1
```

Controller Configuration

```
! Sets authorization to the local radius server
aaa authorization network MLIST_MACFILTER local

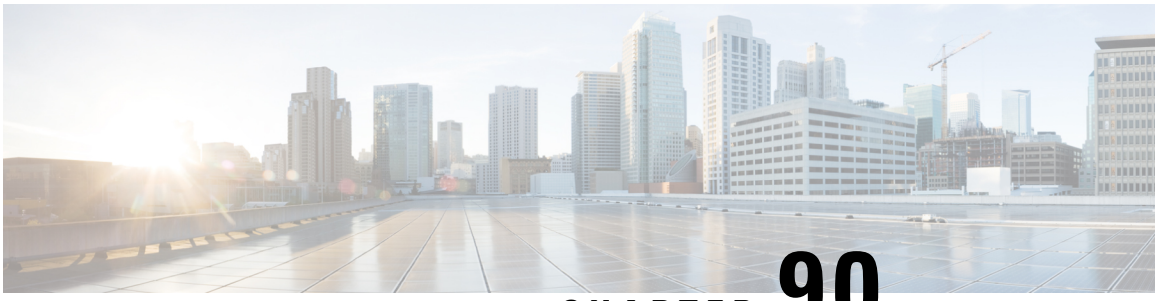
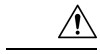
!A WLAN with the SSID WLAN_2 is created and MAC filtering is set along with security
parameters.
wlan WLAN_2 2 WLAN_2
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers

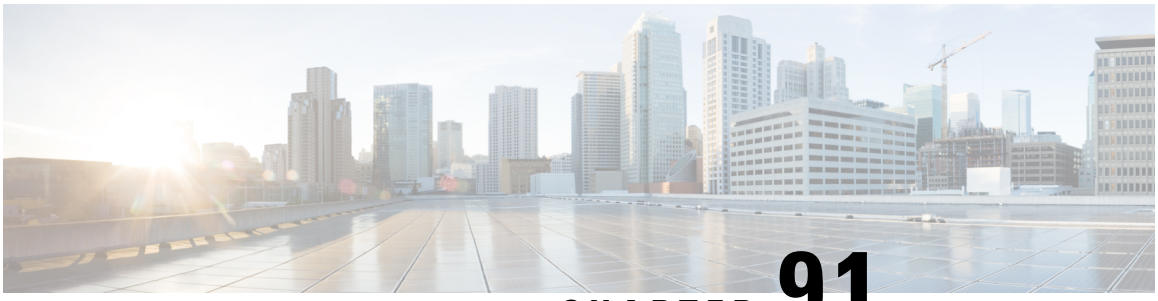
!WLAN with the SSID WLAN_1 is created and MAC filtering is set along with security parameters.
wlan WLAN_1 1 WLAN_1
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list WEBAUTH

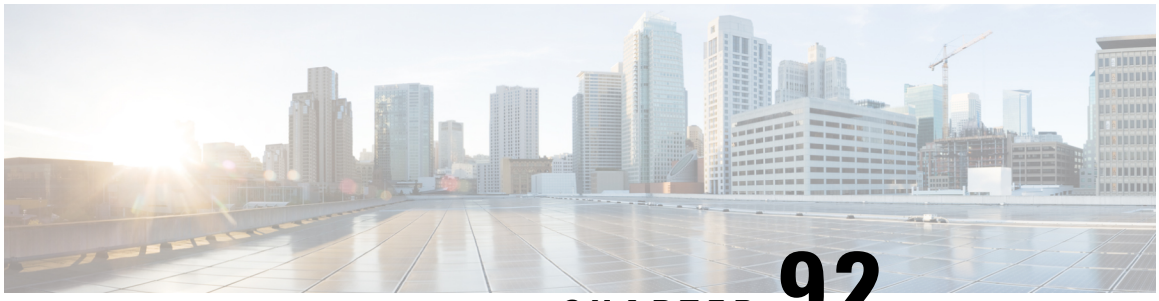
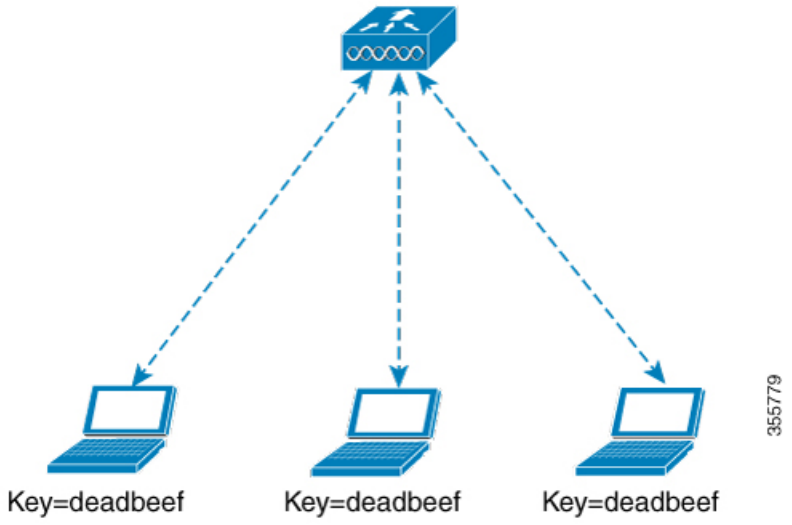
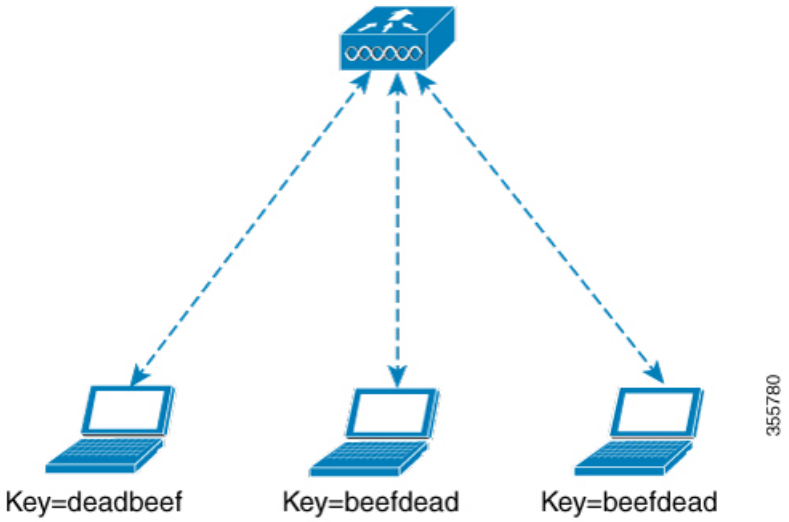
! Policy profile to be associated with the above WLANs
wireless profile policy MAC_FILTER_POLICY
aaa-override
```

```
vlan 504
no shutdown
```

Configuring MAC Filtering for Local Authentication (CLI)

Follow the procedure given below to configure MAB for local authentication.

Before you begin

Configure AAA local authentication.

Configure the username for WLAN configuration (local authentication) using **username** *mac-address* **mac** command.

Note The mac-address must be in the following format: *abcdabcdabcd*

Procedure

	Command or Action	Purpose
Step 1	**wlan** *profile-name wlan-id* **Example:** `wlan CR1_SSID_mab-local-default 1 CR1_SSID_mab-local-default`	Specifies the WLAN name and ID.
Step 2	**mac-filtering default** **Example:** `Device(config-wlan)# mac-filtering default`	Sets MAC filtering support for the WLAN.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA secuirty.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.

	Command or Action	Purpose
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring MAC Filtering (GUI)

Before you begin

Configure AAA external authentication.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLANs**.
Step 2 On the **Wireless Networks** page, click the name of the WLAN.
Step 3 In the **Edit WLAN** window, click the **Security** tab.
Step 4 In the **Layer2** tab, check the **MAC Filtering** check box to enable the feature.
Step 5 With MAC Filtering enabled, choose the **Authorization List** from the drop-down list.
Step 6 Save the configuration.

Configuring MAB for External Authentication (CLI)

Follow the procedure given below to configure MAB for external authentication.

Before you begin

Configure AAA external authentication.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *wlan-name wlan-id ssid-name* **Example:** `wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius`	Specifies the WLAN name and ID.
Step 2	**mac-filtering** *list-name* **Example:** `Device(config-wlan)# mac-filtering ewlc-radius`	Sets the MAC filtering parameters. Here, *ewlc-radius* is an example for the *list-name*

	Command or Action	Purpose
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA secuirty.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**mab request format attribute** {**1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** {**0** | **7** | **LINE**} **LINE** *password* | **32 vlan access-vlan**} **Example:** `Device(config)# mab request format attribute 1 groupsize 4 separator`	Optional. Configures the delimiter while using MAC filtering in a WLAN. Here, **1**- Specifies the username format used for MAB requests. **groupsize** *size*- Specifies the number of hex digits per group. The valid values range from 1 to 12. **separator** *separator*- Specifies how to separate groups. The separators are comma, semicolon, and full stop. **lowercase**- Specifies the username in lowercase format. **uppercase**- Specifies the username in uppercase format. **2**- Specifies the global password used for all the MAB requests. **0**- Specifies the unencrypted password. **7**- Specifies the hidden password. **LINE**- Specifies the encrypted or unencrypted password. *password*- LINE password. **32**- Specifies the NAS-Identifier attribute. **vlan**- Specifies a VLAN. **access-vlan**- Specifies the configured access VLAN.

	Command or Action	Purpose
Step 7	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.



CHAPTER 89

Web-Based Authentication

This chapter describes how to configure web-based authentication on the device. It contains these sections:

- Local Web Authentication Overview, on page 931
- How to Configure Local Web Authentication, on page 939
- Configuration Examples for Local Web Authentication, on page 963
- External Web Authentication (EWA), on page 969
- Authentication for Sleeping Clients, on page 974
- Sleeping Clients with Multiple Authentications, on page 976
- Multi Authentication Combination with 802.1X Authentication and Local Web Authentication, on page 982

Local Web Authentication Overview

Web authentication is a Layer 3 security solution designed for providing easy and secure guest access to hosts on WLAN with open authentication or appropriate layer 2 security methods. Web authentication allows users to get authenticated through a web browser on a wireless client, with minimal configuration on the client side. It allows users to associate with an open SSID without having to set up a user profile. The host receives an IP address and DNS information from the DHCP server, however cannot access any of the network resources until they authenticate successfully. When the host connects to the guest network, the WLC redirects the host to an authentication web page where the user needs to enter valid credentials. The credentials are authenticated by the WLC or an external authentication server and if authenticated successfully is given full access to the network. Hosts can also be given limited access to particular network resources before authentication for which the pre-authentication ACL functionality needs to be configured.

The following are the different types of web authentication methods:

- Local Web Authentication (LWA): Configured as Layer 3 security on the controller, the web authentication page and the pre-authentication ACL are locally configured on the controller. The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server.

- External Web Authentication (EWA): Configured as Layer 3 security on the controller, the controller intercepts htttp(s) traffic and redirects the client to the login page hosted on the external web server. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is configured statically on the controller.

- Central Web Authentication (CWA): Configured mostly as Layer 2 security on the controller, the redirection URL and the pre-authentication ACL reside on ISE and are pushed during layer 2 authentication to the controller. The controller redirects all web traffic from the client to the ISE login page. ISE validates the credentials entered by the client through HTTPS and authenticates the user.

Use the local web authentication feature, known as web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.

When a client initiates an HTTP session, local web authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the local web authentication feature sends to the authentication, authorization, and accounting (AAA) server for authentication.

If authentication succeeds, local web authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

If authentication fails, local web authentication forwards a Login-Fail HTML page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, local web authentication forwards a Login-Expired HTML page to the host, and the user is excluded with the exclusion reason as Web authentication failure.

When a client reaches maximum HTTP connections (maximum of 200 connections when configured), it will cause Transmission Control Protocol (TCP) resets and client exclusion.

Note You should use either global or named parameter-map under WLAN (for method-type, custom, and redirect) for using the same web authentication methods, such as consent, web consent, and webauth. Global parameter-map is applied by default, if none of the parameter-map is configured under WLAN.

Note The traceback that you receive when webauth client tries to do authentication does not have any performance or behavioral impact. It happens rarely when the context for which FFM replied back to EPM for ACL application is already dequeued (possibly due to timer expiry) and the session becomes ‘unauthorized’.

Note When command authorization is enabled as a part of AAA Authorization configuration through TACACS and the corresponding method list is not configured as a part of the HTTP configuration, WebUI pages will not load any data. However, some wireless feature pages may work as they are privilege based and not command based.

Based on where the web pages are hosted, the local web authentication can be categorized as follows:

- *Internal*—The internal default HTML pages (Login, Success, Fail, and Expire) in the controller are used during the local web authentication.
- *Customized*—The customized web pages (Login, Success, Fail, and Expire) are downloaded onto the controller and used during the local web authentication.
- *External*—The customized web pages are hosted on the external web server instead of using the in-built or custom web pages.

Based on the various web authentication pages, the types of web authentication are as follows:

- *Webauth*—This is a basic web authentication. Herein, the controller presents a policy page with the user name and password. You need to enter the correct credentials to access the network.
- *Consent or web-passthrough*—Herein, the controller presents a policy page with the Accept or Deny buttons. You need to click the Accept button to access the network.
- *Webconsent*—This is a combination of webauth and consent web authentication types. Herein, the controller presents a policy page with Accept or Deny buttons along with user name or password. You need to enter the correct credentials and click the Accept button to access the network.

Note

- You can view the webauth parameter-map information using the **show running-config** command output.
- The wireless Web-Authentication feature does not support the bypass type.
- Change in web authentication parameter map redirect login URL does not occur until a AP rejoin happens. You must enable and disable the WLAN to apply the new URL redirection.

Note We recommend that you follow the Cisco guidelines to create a customized web authentication login page. If you have upgraded to the latest versions of Google Chrome or Mozilla Firefox browsers, ensure that your webauth bundle has the following line in the *login.html* file:

```
<body onload="loadAction();">
```

Device Roles

With local web authentication, the devices in the network have these specific roles:

- *Client*—The device (workstation) that requests access to the network and the controller and responds to requests from the controller. The workstation must be running an HTML browser with Java Script enabled.
- *Authentication server*—Authenticates the client. The authentication server validates the identity of the client and notifies the controller that the client is authorized to access the network and the controller services or that the client is denied.
- *Controller*—Controls the physical access to the network based on the authentication status of the client. The controller acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

Figure 25: Local Web Authentication Device Roles



Authentication Process

When the page is hosted on the controller, the controller uses its virtual IP (a non-routable IP like 192.0.2.1 typically) to serve the request. If the page is hosted externally, the web redirection sends the client first to the virtual IP, which then sends the user again to the external login page while it adds arguments to the URL, such as the location of the virtual IP. Even when the page is hosted externally, the user submits its credentials to the virtual IP.

When you enable local web authentication, these events occur:

- The user initiates an HTTP session.
- The HTTP traffic is intercepted, and authorization is initiated. The controller sends the login page to the user. The user enters a username and password, and the controller sends the entries to the authentication server.
- If the authentication succeeds, the controller downloads and activates the user's access policy from the authentication server. The login success page is sent to the user.
- If the authentication fails, the controller sends the login fail page. The user retries the login. If the maximum number of attempts fails, the controller sends the login expired page, and the host is placed in a watch list. After the watch list times out, the user can retry the authentication process.
- If authentication server is not available, after the web authentication retries, the client moves to the excluded state and the client receives an Authentication Server is Unavailable page.
- The controller reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or when the host does not send any traffic within the idle timeout on a Layer 3 interface.
- Web authentication sessions can not apply new VLAN as part of the authorization policy, as the client already has been assigned an IP address and you will not be able to change the IP address in the client, in case the VLAN changes.
- If the terminate action is default, the session is dismantled, and the applied policy is removed.

Note Do not use semicolons (;) while configuring username for GUI access.

Local Web Authentication Banner

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to the controller.

The banner appears on both the login page and the authentication-result pop-up pages. The default banner messages are as follows:

- *Authentication Successful*
- *Authentication Failed*
- *Authentication Expired*

The Local Web Authentication Banner can be configured as follows:

- Use the following global configuration command:

```
Device(config)# parameter map type webauth global
Device(config-params-parameter-map)# banner ?
file <file-name>
text <Banner text>
title <Banner title>
```

The default banner *Cisco Systems* and *Switch host-name Authentication* appear on the Login Page. *Cisco Systems* appears on the authentication result pop-up page.

Figure 26: Authentication Successful Banner

The banner can be customized as follows:

- Add a message, such as switch, router, or company name to the banner:

- New-style mode—Use the following global configuration command:

  parameter-map type webauth global

  banner text <text>

- Add a logo or text file to the banner:
  - New-style mode—Use the following global configuration command:

    parameter-map type webauth global

    banner file <filepath>

Figure 27: Customized Web Banner



If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch.

Figure 28: Login Screen With No Banner



Customized Local Web Authentication

During the local web authentication process, the switch's internal HTTP server hosts four HTML pages to deliver to an authenticating client. The server uses these pages to notify you of these four authentication process states:

- Login: Your credentials are requested
- Success: The login was successful
- Fail: The login failed
- Expire: The login session has expired because of excessive login failures

Note Virtual IP address is mandatory to configure custom web authentication.

From Cisco IOS XE Dublin 17.11.1, special characters such as *ö* or *à* are supported in the login portal for banner title and banner text. The number of characters supported on the banner text has been doubled to 400. To support special characters, ensure that you configure the **exec-character-bits** command under the line console (for serial port) or line vty (for SSH).

Note

- If the banner text string exceeds the maximum limit of 400 characters, an error message is displayed and the configuration is rejected. Also, the parser has a limitation of 254 characters per line (including the CLI keywords). If you want to use more than 254 characters, ensure that you split it into two or multiple lines.
- The webauth login page displays only the default banner strings if banner command is not configured.

Guidelines

- You can substitute your own HTML pages for the default internal HTML pages.
- You can use a logo or specify text in the *login*, *success*, *failure*, and *expire* web pages.
- On the banner page, you can specify text in the login page.
- The pages are in HTML.
- You must include an HTML redirect command in the success page to access a specific URL.
- The URL string must be a valid URL (for example, http://www.cisco.com). An incomplete URL might cause *page not found* or similar errors on a web browser.
- If you configure web pages for HTTP authentication, they must include the appropriate HTML commands (for example, to set the page time out, to set a hidden password, or to confirm that the same page is not submitted twice). The custom page samples in the webauth bundle are provided with the image and the details of what you can and cannot change.
- The CLI command to redirect users to a specific URL is not available when the configured login form is enabled. The administrator should ensure that the redirection is configured in the web page.
- If the CLI command redirecting users to specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI command redirecting users to a specific URL does not take effect.
- Configured web pages can be copied to the switch boot flash or flash.
- The login page can be on one flash, and the success and failure pages can be another flash (for example, the flash on the active switch or a member switch).
- You must configure all four pages.
- All of the logo files (image, flash, audio, video, and so on) that are stored in the system directory (for example, flash, disk0, or disk) and that are displayed on the login page must use *web_auth_<filename>* as the file name.
- The configured authentication proxy feature supports both HTTP and SSL.

You can substitute your HTML pages for the default internal HTML pages. You can also specify a URL to which users are redirected after authentication occurs, which replaces the internal Success page.

Figure 29: Customizable Authentication Page



Redirection URL for Successful Login Guidelines

When configuring a redirection URL for successful login, consider these guidelines:

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and is not available in the CLI. You can perform redirection in the custom-login success page.
- If the redirection URL feature is enabled, a configured auth-proxy-banner is not used
- To remove the specification of a redirection URL, use the **no** form of the command.
- If the redirection URL is required after the web-based authentication client is successfully authenticated, then the URL string must start with a valid URL (for example, http://) followed by the URL information. If only the URL is given without http://, then the redirection URL on successful authentication might cause page not found or similar errors on a web browser.

How to Configure Local Web Authentication

Configuring Default Local Web Authentication

The following table shows the default configurations required for local web authentication.

Table 70: Default Local Web Authentication Configuration

Feature	Default Setting
AAA	Disabled

Feature	Default Setting
RADIUS server • IP address • UDP authentication port • Key	• None specified
Default value of inactivity timeout	3600 seconds
Inactivity timeout	Disabled

Information About the AAA Wizard

The AAA wizard helps you to add the authentication, authorization, and accounting details without having to access multiple windows.

Note When command authorization is enabled as a part of AAA Authorization configuration through TACACS and the corresponding method list is not configured as a part of the HTTP configuration, WebUI pages will not load any data. However, some wireless feature pages may work as they are privilege-based and not command based.

Note Note the following limitations for a TACACS+ user on the 9800 WebUI:

- Users with privilege level 1-10 can only view the **Monitor** tab.
- Users with privilege level 15 have full access.
- Users with privilege level 15 and a command set allowing specific commands only, is not supported.

Note When you configure the AAA authentication and authorization attributes, the following format must be followed:

- protocol:attr=bla
- protocol:attr#0=bla
- protocol:attr#*=bla
- attr=bla
- attr#0=bla
- attr#*=bla

attr is mapped to the supported AAA attributes. If *attr* is an unknown or undefined attribute, a warning message *parse unknown cisco vsa* is displayed when you configure the **radius-server disallow unknown vendor-code** command. Otherwise, the transaction will be treated as a failure.

We recommend that you configure the command as per the format discussed above. Otherwise, the transaction fails. Whenever the passed attribute does not match any of the patterns mentioned, then AAA fails to decode that specific attribute and marks the request as a failure.

To edit the details entered using the wizard, use the respective screens.

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**.

Step 2 Click + **AAA Wizard**.

The **Add Wizard** page is displayed.

Step 3 Click **RADIUS** tab.

The RADIUS server option is enabled by default. You can switch between the **Basic** and **Advanced** options using the radio buttons.

a) In the **Name** field, enter the name of the RADIUS server.
b) In the **IPv4 / IPv6 Server Address** field, enter the IPv4 or IPv6 address, or hostname.
c) Check the **PAC Key** check box to enable the Protected Access Credential (PAC) authentication key option.
d) From the **Key Type** drop-down list, choose the authentication key type.
e) In the **Key** field, enter the authentication key.
f) In the **Confirm Key** field, re-enter the authentication key.
g) Click the **Advanced** radio button.

This enables the **Advanced** options.

h) In the **Auth Port** field, enter the authorization port number.
i) In the **Acct Port** field, enter the accounting port number.
j) In the **Server Timeout** field, enter the timeout duration, in seconds.
k) In the **Retry Count** field, enter the number of retries.

l) Use the **Support for CoA** toggle button to enable or disable change of authorization (CoA).

Step 4 Check the **TACACS+** check box.

This enables the TACACS+ options. You can switch between the **Basic** and **Advanced** options using the radio buttons.

a) In the **Name** field, enter the TACACS+ server name.
b) In the **IPv4 / IPv6 Server Address** field, enter the IPv4 or IPv6 address, or hostname.
c) In the **Key** field, enter the authentication key.
d) In the **Confirm Key** field, re-enter the authentication key.
e) Click the **Advanced** radio button.

This enables the **Advanced** options.

f) In the **Port** field, enter the port number to use.
g) In the **Server Timeout** field, enter the timeout duration, in seconds.

Step 5 Check the **LDAP** check box.

This enables the LDAP options. You can switch between the **Basic** and **Advanced** options using the radio buttons.

a) In the Server Name field, enter the **LDAP** server name.
b) In the **IPv4 / IPv6 Server Address** field, enter the IPv4 or IPv6 address, or hostname.
c) In the **Port Number** field, enter the port number to use.
d) From the **Simple Bind** drop-down list, choose the authentication key type.
e) In the **User Base DN** field, enter the details.
f) Click the **Advanced** radio button.

This enables the **Advanced** options.

g) From the **User Attribute** drop-down list, choose the user attribute.
h) In the **User Object Type** field, enter the object type details and click the + icon.

The objects that have been added are listed in the area below. Use the x mark adjacent to each object to remove it.

i) In the **Server Timeout** field, enter the timeout duration, in seconds.
j) Check the **Secure Mode** check box to enable secure mode.

Checking this enables the **Trustpoint Name** drop-down list.

k) From the **Trustpoint Name** drop-down list, choose the trustpoint.
l) Click **Next**.

This enables the **Server Group Association** page and the RADIUS tab is selected by default.

Step 6 Perform the following actions under **RADIUS** tab.

a) In the **Name** field, enter the name of the RADIUS server group.
b) From the **MAC-Delimiter** drop-down list, choose the delimiter to be used in the MAC addresses that are sent to the RADIUS servers.
c) From the **MAC Filtering** drop-down list, choose a value based on which to filter MAC addresses.
d) To configure the dead time for the server group and direct AAA traffic to alternative groups of servers that have different operational characteristics, in the **Dead-Time** field, enter the amount of time, in minutes, after which a server is assumed to be dead.

e) Choose the servers that you want to include in the server group from the **Available Servers** list and move them to the **Assigned Servers** list.
f) Click **Next**.

The **TACACS+** window is displayed, if you have selected **TACACS+** in server configuration.

Step 7 Use the **TACACS+** window to enter the following details:

a) In the **Name** field, enter the name of the TACACS+ server group.
b) From the **Available Servers** list, choose the servers that you want to include in the server group from the list and move them to the **Assigned Servers** list.
c) Click **Next**.

The **LDAP** window is displayed, if you have selected **LDAP** under server configuration.

Step 8 Use the **LDAP** window to enter the following details:

a) In the **Name** field, enter the name of the LDAP server group.
b) From the **Available Servers** list, choose the servers that you want to include in the server group from the list and move them to the **Assigned Servers** list.

Step 9 Click **Next**.

The **MAP AAA** window is displayed.

Use the check boxes to enable the **Authentication**, **Authorization**, and **Accounting** tabs. You cannot unselect all the three options. At least one option has to be selected.

Step 10 Use the **Authentication** tab to enter the authentication details:

a) In the **Method List Name** field, enter the name of the method list.
b) From the **Type** drop-down list, choose the type of accounting that you want to perform before allowing access to the network.
c) From the **Group Type** drop-down list, choose a value depending on whether you want to assign a group of servers as your access server, or want to use a local server to authenticate access.

If you choose the local option, the **Fallback** to local option is removed.

d) Check the **Fallback to local** check box to configure a local server to act as a fallback method when servers in the group are unavailable.
e) From the **Available Server Groups** list, choose the server groups that you want to use to authenticate access to your network and click the > icon to move them to the **Assigned Server Groups** list.

Step 11 Check the **Authorization** check box to configure the authorization details:

a) In the **Method List Name** field, enter the name of the method list.
b) From the **Type** drop-down list, choose the type of authorization you want to perform before allowing access to the network.
c) From the **Group Type** drop-down list, choose a value depending on whether you want to assign a group of servers as your access server, or want to use a local server to authorize access.

If you choose the local option, the **Fallback** to local option is removed.

d) Check the **Fallback to local** check box to configure a local server to act as a fallback method when the servers in the group are unavailable.
e) From the **Available Server Groups** list, choose the server groups you want to use to authorize access to your network and click > icon to move them to the **Assigned Server Groups** list.

Step 12 Check the **Accounting** check box to configure the accounting details:

a) In the **Method List Name** field, enter the name of the method list.
b) From the **Type** drop-down list, choose the type of accounting that you want to perform.
c) From the **Available Server Groups** list, choose the server groups that you want to use to authorize access to your network and click the > icon to move them to the **Assigned Server Groups** list.

Step 13 Click **Apply to Device**.

Configuring AAA Authentication (GUI)

Note The WebUI does not support the ipv6 radius source-interface under AAA radius server group configuration.

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**.

Step 2 In the **Authentication** section, click **Add**.

Step 3 In the **Quick Setup: AAA Authentication** window that is displayed, enter a name for your method list.

Step 4 Choose the type of authentication you want to perform before allowing access to the network, in the **Type** drop-down list.

Step 5 Choose if you want to assign a group of servers as your access server, or if you want to use a local server to authenticate access, from the **Group** Type drop-down list.

Step 6 To configure a local server to act as a fallback method when servers in the group are unavailable, check the **Fallback** to local check box.

Step 7 Choose the server groups you want to use to authenticate access to your network, from the **Available Server Groups** list and click > icon to move them to the **Assigned Server Groups** list.

Step 8 Click **Save & Apply to Device**.

Configuring AAA Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA functionality.

	Command or Action	Purpose
Step 2	**aaa authentication login** {**default** | *named_authentication_list*} **group** *AAA_group_name* **Example:** `Device(config)# aaa authentication login default group group1`	Defines the list of authentication methods at login. **named_authentication_list** refers to any name that is not greater than 31 characters. **AAA_group_name** refers to the server group name. You need to define the server-group **server_name** at the beginning itself.
Step 3	**aaa authorization network** {**default** | **named**} **group** *AAA_group_name* **Example:** `Device(config)# aaa authorization network default group group1`	Creates an authorization method list for web-based authorization.
Step 4	**tacacs server** *server-name* **Example:** `Device(config)# tacacs server yourserver`	Specifies an AAA server.
Step 5	**address** {**ipv4** | **ipv6**}*ip_address* **Example:** `Device(config-server-tacacs)# address ipv4 10.0.1.12`	Configures the IP address for the TACACS server.
Step 6	**single-connection** **Example:** `Device(config-server-tacacs)# single-connection`	Multiplexes all packets over a single TCP connection to TACACS server.
Step 7	**tacacs-server host** {*hostname* | *ip_address*} **Example:** `Device(config)# tacacs-server host 10.1.1.1`	Specifies a AAA server.

Configuring the HTTP/HTTPS Server (GUI)

Procedure

Step 1 Choose **Administration** > **Management** > **HTTP/HTTPS/Netconf**.

Step 2 In the **HTTP/HTTPS Access Configuration** section, enable HTTP Access and enter the port that will listen for HTTP requests. The default port is 80. Valid values are 80, and ports between 1025 and 65535.

Step 3 Enable **HTTPS Access** on the device and enter the designated port to listen for HTTPS requests. The default port is 1025. Valid values are 443, and ports between 1025 and 65535. On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser.

Step 4 Choose the **Personal Identity Verification** as enabled or disabled.

Step 5 In the **HTTP Trust Point Configuration** section, enable **Enable Trust Point** to use Certificate Authority servers as trustpoints.

Step 6 From the **Trust Points** drop-down list, choose a trust point.

Step 7 In the **Timeout Policy Configuration** section, enter the HTTP timeout policy in seconds. Valid values can range from 1 to 600 seconds.

Step 8 Enter the number of minutes of inactivity allowed before the session times out. Valid values can range from 180 to 1200 seconds.

Step 9 Enter the server life time in seconds. Valid values can range from 1 to 86400 seconds.

Step 10 Enter the maximum number of requests the device can accept. Valid values range from 1 to 86400 requests.

Step 11 Save the configuration.

Configuring the HTTP Server (CLI)

To use local web authentication, you must enable the HTTP server within the device. You can enable the server for either HTTP or HTTPS.

Note The Apple psuedo-browser will not open if you configure only the **ip http secure-server** command. You should also configure the **ip http server** command.

Follow the procedure given below to enable the server for either HTTP or HTTPS:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server. The local web authentication feature uses the HTTP server to communicate with the hosts for user authentication.
Step 3	**ip http secure-server** **Example:** `Device(config)# ip http secure-server`	Enables HTTPS. You can configure custom authentication proxy web pages or specify a redirection URL for successful login. **Note** To ensure secure authentication when you enter the **ip http secure-server** command, the login page is always in HTTPS (secure HTTP) even if the user sends an HTTP request.
Step 4	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Allowing Special Characters for Serial Port

Before you begin

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**line console** *line-num* **Example:** `Device(config)# line console 0`	Configures the primary terminal line number.
Step 3	**exec-timeout** *mins sec* **Example:** `Device(config-line)# exec-timeout 12 0`	Configures the time to disconnect idle EXEC sessions.

	Command or Action	Purpose
Step 4	**login authentication** *word* **default** **Example:** `Device(config-line)# login authentication NO_LOGIN`	Configures login authentication checking. It can be authentication list with a name or the default authentication list.
Step 5	**exec-character-bit** {**7** | **8**} **Example:** `Device(config-line)# exec-character-bit 8`	Configures the character widths of EXEC command characters.
Step 6	**stopbits** {**1** | **1.5** | **2**} **Example:** `Device(config-line)# stopbits 1`	Configures the stop bits for the console port.
Step 7	**end** **Example:** `Device(config-line)# end`	Returns to privileged EXEC mode.

Allowing Special Characters for VTY Port

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 3	**banner text** *text* **Example:** `Device(config-params-parameter-map)# banner text #Hêllö#`	You can create a custom banner (of up to 400 characters) by entering *c* <*banner-text*> *c*, where *c* is a delimiting character. If the string exceeds the maximum limit of 400 characters, an error message is displayed and the configuration is rejected. Also, the parser has a limitation of 254 characters per line (including the CLI keywords). If you want to use more than 254 characters, ensure that you split it into two or multiple lines.

	Command or Action	Purpose
		The webauth login page displays only the default banner strings, if banner command is not configured.
Step 4	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring HTTP and HTTPS Requests for Web Authentication

Information About Configuring HTTP and HTTPS Requests for Web Authentication

Using the Configuring HTTP and HTTPS Requests for Web Authentication feature, you can have HTTPS access to device management and HTTP access to web authentication. To control the HTTP and HTTPS requests being sent to the web authentication module, run the **secure-webauth-disable** and **webauth-http-enable** commands in the global parameter map mode.

Note The **secure-webauth-disable** and **webauth-http-enable** commands are not enabled by default; you must configure them explicitly.

The following table describes the various CLI combinations:

Table 71: CLI Combinations

Admin (Device Management)		WebAuthentication		Required Configurations	
HTTP Access	**HTTPS Access**	**HTTP Access**	**HTTPS Access**	**Admin**	**Web Authentication**

No	Yes	Yes	Yes	`no ip http server`
				`ip http secure-server`
					`no ip http server`
					`ip http secure-server`
					`parameter-map type webauth global`
					`webauth-http-enable`

No	Yes	No	Yes	`no ip http server` `ip http secure-server`	`no ip http server` `ip http secure-server`

Admin (Device Management)		WebAuthentication		Required Configurations	
HTTP Access	**HTTPS Access**	**HTTP Access**	**HTTPS Access**	**Admin**	**Web Authentication**

No	Yes	Yes	No	`no ip http server`
				`ip http secure-server`
					`no ip http server`
					`ip http secure-server`
					
					`parameter-map type webauth global`
					
					`webauth-http-enable`
					
					`secure-webauth-disable`

No	Yes	No	No	`no ip http server`
				`ip http secure-server`
					`no ip http server`
					`ip http secure-server`
					
					`parameter-map type webauth global`
					
					`secure-webauth-disable`

No	No	No	Yes	`no ip http server` `no ip http secure-server`	Not Supported

No	No	Yes	No	`no ip http server`
				`no ip http secure-server`
					`no ip http server`
					`no ip http secure-server`
					
					`parameter-map type webauth global`
					
					`webauth-http-enable`

Yes	No	Yes	No	`ip http server` `no ip http secure-server`	`ip http server` `no ip http secure-server`

Yes	Yes	Yes	No	`ip http server`
				`ip http secure-server`
					`ip http server`
					`ip http secure-server`
					
					`parameter-map type webauth global`
					
					`secure-webauth-disable`

Note

- The **ip http server** and **ip http secure-server** commands allow access for HTTP and HTTPS, respectively. For example, in the first row of the table, for HTTP access to web authentication, you do not require the **ip http server** command. You can use the new **webauth-http-enable** command under the global parameter map, to allow HTTP access.
- For HTTPS access to webauth, the **ip http secure-server** command is required. Therefore, HTTPS access for both admin and web authentication are enabled in the first row. To disable HTTPS access for web authentication, configure the **secure-webauth-disable** command. For example, in the fourth row of the table, HTTPS access is disabled for web authentication because the **secure-webauth-disable** command is configured.

Guidelines and Limitations

The following are the guidelines and limitations for configuring HTTP and HTTPS requests for web authentication:

- You cannot enable HTTPS web authentication without enabling HTTPS for device management.
- If the **secure-webauth-disable** command is configured, central web authentication cannot be performed, if the initial request from the client is https://< >.

Configuring HTTP and HTTPS Requests for Web Authentication (CLI)

To configure the HTTP and HTTPS requests being sent to the webauth module, complete the steps given below:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no ip http server** **Example:** `Device(config)# no ip http server`	Sets the HTTP server to its default.
Step 4	**ip http** {**server** | **secure-server**} **Example:** `Device(config)# ip http server`	Enables the HTTP server or the HTTP secure server.

	Command or Action	Purpose
Step 5	**parameter-map type webauth global** **Example:** `Device(config)# parameter-map type webauth global`	Enables the global parameter map mode.
Step 6	**secure-webauth-disable** **Example:** `Device(config-params-parameter-map)# secure-webauth-disable`	Disables HTTP secure server for web authentication.
Step 7	**webauth-http-enable** **Example:** `Device(config-params-parameter-map)# webauth-http-enable`	Enables HTTP server for web authentication.

Creating a Parameter Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 Click **Add**.

Step 3 Click **Policy Map**.

Step 4 Enter **Parameter Name**, **Maximum HTTP connections**, **Init-State Timeout(secs)** and choose **webauth** in the **Type** drop-down list.

Step 5 Click **Apply to Device**.

Creating Parameter Maps

Configuring Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 On the **Web Auth** page, click **Add**.

Step 3 In the **Create Web Auth Parameter** window that is displayed, enter a name for the parameter map.

Step 4 In the **Maximum HTTP Connections** field, enter the maximum number of HTTP connections that you want to allow.

Step 5 In the **Init-State Timeout** field, enter the time after which the init state timer should expire due to user's failure to enter valid credentials in the login page.

Step 6 Choose the type of Web Auth parameter.

Step 7 Click **Apply to Device**.

Step 8 On the **Web Auth** page, click the name of the parameter map.

Step 9 In the **Edit WebAuth Parameter** window that is displayed, choose the required **Banner Type**.

- If you choose **Banner Text**, enter the required banner text to be displayed.
- If you choose **File Name**, specify the path of the file from which the banner text has to be picked up.

Step 10 Enter the virtual IP addresses as required.

Step 11 Set appropriate status of **WebAuth Intercept HTTPS**, **Captive Bypass Portal**.

Step 12 Set appropriate status for **Disable Success Window**, **Disable Logout Window**, and **Login Auth Bypass for FQDN**.

Step 13 Check the **Sleeping Client Status** check box to enable authentication of sleeping clients and then specify the **Sleeping Client Timeout** in minutes. Valid range is between 10 minutes and 43200 minutes.

Step 14 Click the **Advanced** tab.

Step 15 To configure external web authentication, perform these tasks:

a) In the **Redirect for log-in** field, enter the name of the external server to send login request.
b) In the **Redirect On-Success** field, enter the name of the external server to redirect after a successful login.
c) In the **Redirect On-Failure** field, enter the name of the external server to redirect after a login failure.
d) (Optional) Under **Redirect to External Server** in the **Redirect Append for AP MAC Address** field, enter the AP MAC address.
e) (Optional) In the **Redirect Append for Client MAC Address** field, enter the client MAC address.
f) (Optional) In the **Redirect Append for WLAN SSID** field, enter the WLAN SSID.
g) In the **Portal IPV4 Address** field, enter the IPv4 address of the portal to send redirects.
h) In the **Portal IPV6 Address** field, enter the IPv6 address of the portal to send redirects, if IPv6 address is used.

Step 16 To configure customized local web authentication, perform these tasks:

a) Under **Customized Page**, specify the following pages:

- **Login Failed Page**
- **Login Page**
- **Logout Page**
- **Login Successful Page**

Step 17 Click **Update & Apply**.

Configuring the Internal Local Web Authentication (CLI)

Follow the procedure given below to configure the internal local web authentication:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** {*parameter-map-name* | **global**} **Example:** `Device(config)# parameter-map type webauth sample`	Creates the parameter map. The **parameter-map-name** must not exceed 99 characters.
Step 3	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring the Customized Local Web Authentication (CLI)

Follow the procedure given below to configure the customized local web authentication:

Note Virtual IP address is mandatory for custom web authentication.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth sample`	Configures the webauth type parameter. **Note** You need to configure a virtual IP in the global parameter map to use the customized web authentication bundle.
Step 3	**type** {**authbypass** | **consent** | **webauth** | **webconsent**} **Example:**	Configures webauth sub-types, such as passthru, consent, webauth, or webconsent.

	Command or Action	Purpose
	`Device(config-params-parameter-map)# type webauth`	
Step 4	**custom-page login device** *html-filename* **Example:** `Device(config-params-parameter-map)# custom-page login device bootflash:login.html`	Configures the customized login page.
Step 5	**custom-page login expired device** *html-filename* **Example:** `Device(config-params-parameter-map)# custom-page login expired device bootflash:loginexpired.html`	Configures the customized login expiry page.
Step 6	**custom-page success device** *html-filename* **Example:** `Device(config-params-parameter-map)# custom-page success device bootflash:loginsuccess.html`	Configures the customized login success page.
Step 7	**custom-page failure device** *html-filename* **Example:** `Device(config-params-parameter-map)# custom-page failure device bootflash:loginfail.html`	Configures the customized login failure page.
Step 8	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring the External Local Web Authentication (CLI)

Follow the procedure given below to configure the external local web authentication:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth sample`	Configures the webauth type parameter.
Step 3	**type** {**authbypass** | **consent** | **webauth** | **webconsent**} **Example:** `Device(config-params-parameter-map)# type webauth`	Configures the webauth sub-types, such as authbypass, consent, passthru, webauth, or webconsent.
Step 4	**redirect** [**for-login** | **on-failure** | **on-success**] *URL* **Example:** `Device(config-params-parameter-map)# redirect for-login http://www.cisco.com/login.html`	Configures the redirect URL for the login, failure, and success pages. **Note** In the redirect url, you need to press *Ctrl+v* and type *?* to configure the *?* character. The *?* character is commonly used in URL when ISE is configured as an external portal.
Step 5	**redirect portal** {**ipv4** | **ipv6**} *ip-address* **Example:** `Device(config-params-parameter-map)# redirect portal ipv4 23.0.0.1`	Configures the external portal IPv4 address. **Note** The IP address should be one of the associated IP addresses of the domain and not a random IP address when using FQDN. It is recommended to use the FQDN URL here, if a given domain resolves to more than a single IP address.
Step 6	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring the Web Authentication WLANs

Follow the procedure given below to configure WLAN using web auth security and map the authentication list and parameter map:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID. *profile-name* is the WLAN name which can contain 32 alphanumeric characters. *wlan-id* is the wireless LAN identifier. The valid range is from 1 to 512. *ssid-name* is the SSID which can contain 32 alphanumeric characters.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables the WPA security.
Step 4	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for WLAN.

Step 5	**security web-auth** {**authentication-list** *authentication-list-name* | **parameter-map** *parameter-map-name*}
	Example:
	`Device(config-wlan)# security web-auth authentication-list webauthlistlocal`
	`Device(config-wlan)# security web-auth parameter-map sample`
		Enables web authentication for WLAN.
		Here,
		• **authentication-list** *authentication-list-name*: Sets the authentication list for IEEE 802.1x.
		• **parameter-map** *parameter-map-name*: Configures the parameter map.

	Command or Action	Purpose
		Note When **security web-auth** is enabled, you get to map the default **authentication-list** and global **parameter-map**. This is applicable for authentication-list and parameter-map that are not explicitly mentioned.
Step 6	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Pre-Auth Web Authentication ACL (GUI)

Before you begin

Ensure that you have configured an access control list (ACL) and a WLAN.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 Click the name of the WLAN.
Step 3 In the **Edit WLAN** window, click the **Security** tab and then click the **Layer3** tab.
Step 4 Click **Show Advanced Settings**.
Step 5 In the **Preauthenticaion ACL** section, choose the appropriate ACL to be mapped to the WLAN.
Step 6 Click **Update & Apply to Device**.

Configuring Pre-Auth Web Authentication ACL (CLI)

Follow the procedure given below to configure pre-auth web authentication ACL:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**access-list** *access-list-number* {**deny** | **permit**} *hostname source-wildcard-bits* **Example:** `Device(config)# access-list 2 deny your_host 10.1.1.1 log`	Creates an ACL list. The *access-list-number* is a decimal number from 1 to 99, 100 to 199, 300 to 399, 600 to 699, 1300 to 1999, 2000 to 2699, or 2700 to 2799. Enter **deny** or **permit** to specify whether to deny or permit if the conditions are matched. The *source* is the source address of the network or host from which the packet is being sent specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. • The keyword **host** as an abbreviation for *source* and *source-wildcard* of source 0.0.0.0. (Optional) The *source-wildcard* applies wildcard bits to the source.
Step 3	**wlan** *profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Creates the WLAN. *profile-name* is the WLAN name which can contain 32 alphanumeric characters. *wlan-id* is the wireless LAN identifier. The valid range is from 1 to 512. *ssid-name* is the SSID which can contain 32 alphanumeric characters.
Step 4	**ip access-group web** *access-list-name* **Example:** `Device(config-wlan)# ip access-group web name`	Maps the ACL to the web auth WLAN. *access-list-name* is the IPv4 ACL name or ID.
Step 5	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring the Maximum Web Authentication Request Retries

Follow these steps to configure the maximum web authentication request retries:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless security web-auth retries** *number* **Example:** `Device(config)# wireless security web-auth retries 2`	*number* is the maximum number of web auth request retries. The valid range is 0 to 20.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring a Local Banner in Web Authentication Page (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

Step 3 In the **General** tab and choose the required Banner Type:

- If you choose **Banner Text**, enter the required banner text to be displayed.
- If you choose **File Name**, specify the path of the file from which the banner text has to be picked up.

Step 4 Click **Update & Apply**.

Configuring a Local Banner in Web Authentication Page (CLI)

Follow the procedure given below to configure a local banner in web authentication pages.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *param-map* **Example:** `Device(config)# parameter-map type webauth param-map`	Configures the web authentication parameters. Enters the parameter map configuration mode.
Step 3	**banner** [*file* | *banner-text* | *title*] **Example:** `Device(config-params-parameter-map)# banner http C My Switch C`	Enables the local banner. Create a custom banner by entering *C banner-text C* (where *C* is a delimiting character), or *file* that indicates a file (for example, a logo or text file) that appears in the banner, or *title* that indicates the title of the banner.
Step 4	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring Type WebAuth, Consent, or Both

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map name* **Example:** `Device (config)  # parameter-map type webauth webparalocal`	Configures the webauth type parameter.

	Command or Action	Purpose
Step 3	**type consent** **Example:** `Device (config-params-parameter-map) # type consent`	Configures webauth type as consent. You can configure the type as webauth, consent, or both (webconsent).
Step 4	**end** **Example:** `Device (config-params-parameter-map) # end`	Returns to privileged EXEC mode.
Step 5	**show running-config | section parameter-map type webauth** *parameter-map* **Example:** `Device (config) # show running-config | section parameter-map type webauth test`	Displays the configuration details.

Configuring Preauthentication ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Device (config)# wlan ramban`	For *wlan-name*, enter the profile name.
Step 3	**shutdown** **Example:** `Device (config-wlan)# shutdown`	Disables the WLAN.
Step 4	**ip access-group web** *preauthrule* **Example:** `Device (config-wlan)# ip access-group web preauthrule`	Configures ACL that has to be applied before authentication.
Step 5	**no shutdown** **Example:** `Device (config)# no shutdown`	Enables the WLAN.
Step 6	**end**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device (config-wlan)# end`	
Step 7	**show wlan name** *wlan-name* **Example:** `Device# show wlan name ramban`	Displays the configuration details.

Configuring TrustPoint for Local Web Authentication

Before you begin

Ensure that a certificate is installed on your controller . Using trustpoint controller presents the domain specific certificate that client browser trusts when it gets redirected to ***.com** portal.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Device (config)# parameter-map type webauth global`	Creates the parameter map.
Step 3	**trustpoint** *trustpoint-name* **Example:** `Device (config-params-parameter-map)# trustpoint trustpoint-name`	Configures trustpoint for local web authentication.
Step 4	**end** **Example:** `Device (config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuration Examples for Local Web Authentication

Example: Obtaining Web Authentication Certificate

This example shows how to obtain web authentication certificate.

```
Device# configure terminal
Device(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Device(config)# end
Device# show crypto pki trustpoints cert
 Trustpoint cert:
    Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
          Serial Number (hex): 00
    Certificate configured.
Device# show  crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Validity Date:
```

```
    start date: 07:27:56 UTC Jan 31 2012
    end   date: 07:27:56 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12 ldap
  Storage: nvram:rkannajrcisc#0CA.cer
```

Example: Displaying a Web Authentication Certificate

This example shows how to display a web authentication certificate.

```
Device# show crypto ca certificate verb
     Certificate
     Status: Available
     Version: 3
     Certificate Serial Number (hex): 2A9636AC00000000858B
     Certificate Usage: General Purpose
     Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
    Subject:
    Name: WS-C3780-6DS-S-2037064C0E80
    Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
    cn=WS-C3780-6DS-S-2037064C0E80
    serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
    CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/cmca.crl
    Validity Date:
    start date: 15:43:22 UTC Aug 21 2011
    end   date: 15:53:22 UTC Aug 21 2021
    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
    Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
    X509v3 extensions:
    X509v3 Key Usage: F0000000
      Digital Signature
      Non Repudiation
      Key Encipherment
      Data Encipherment
    X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
    X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
    Authority Info Access:
    Associated Trustpoints: CISCO_IDEVID_SUDI
    Key Label: CISCO_IDEVID_SUDI
```

Example: Choosing the Default Web Authentication Login Page

This example shows how to choose a default web authentication login page.

```
Device# configure terminal
Device(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL
control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
```

```
Device(config)# wlan wlan50
Device(config-wlan)# shutdown
Device(config-wlan)# security web-auth authentication-list test
Device(config-wlan)# security web-auth parameter-map test
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show running-config | section wlan50
wlan wlan50 50 wlan50
 security wpa akm cckm
 security wpa wpa1
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security web-auth authentication-list test
 security web-auth parameter-map test
 session-timeout 1800
 no shutdown

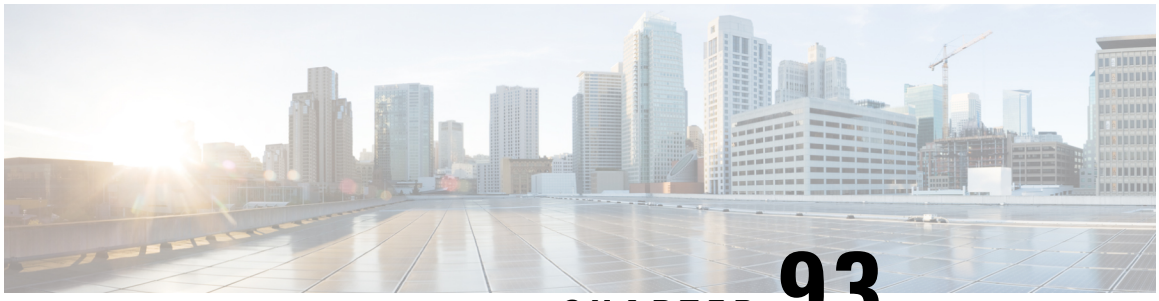
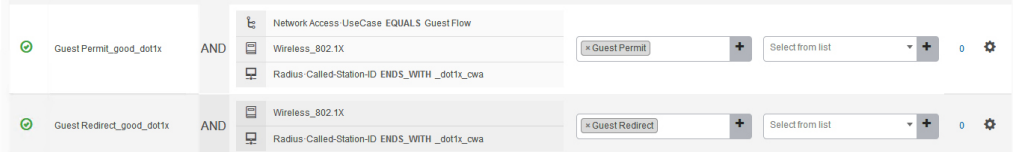
Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
 type webauth
```

Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server

This example shows how to choose a customized web authentication login page from an IPv4 external web server.

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1.
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Device(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 192.0.2.1.
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

Example: Choosing a Customized Web Authentication Login Page from an IPv6 External Web Server

This example shows how to choose a customized web authentication login page from an IPv6 external web server.

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv6 2001:DB8::/48
Device(config-params-parameter-map)# parameter-map type webauth test
```

```
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9:1:1::100/login.html
Device(config-params-parameter-map)# redirect portal ipv6 9:1:1::100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv6 2001:DB8::/48
parameter-map type webauth test
type webauth
redirect for-login http://9:1:1::100/login.html
redirect portal ipv6 9:1:1::100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

Example: Assigning Login, Login Failure, and Logout Pages per WLAN

This example shows how to assign login, login failure and logout pages per WLAN.

```
Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Device(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
Device(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Device(config-params-parameter-map)# custom-page success device flash:loginsucess.html
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
 custom-page login device flash:loginsantosh.html
 custom-page success device flash:loginsucess.html
 custom-page failure device flash:loginfail.html
 custom-page login expired device flash:loginexpire.html
```

Example: Configuring Preauthentication ACL

This example shows how to configure preauthentication ACL.

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show wlan name fff
```

Example: Configuring Webpassthrough

This example shows how to configure webpassthrough.

```
Device# configure terminal
Device(config)# parameter-map type webauth webparalocal
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# end
```

```
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
```

Verifying Web Authentication Type

To verify the web authentication type, run the following command:

```
Device# show parameter-map type webauth all
Type Name
---------------------------------
Global global
Named webauth
Named ext
Named redirect
Named abc
Named glbal
Named ewa-2
```

```
Device# show parameter-map type webauth global
Parameter Map Name : global
Banner:
Text : CisCo
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Enabled
Sleeping-Client timeout : 60 min
Virtual-ipv4 : 192.0.2.1.
Virtual-ipv4 hostname :
Webauth intercept https : Disabled
Webauth Captive Bypass : Disabled
Webauth bypass intercept ACL :
Trustpoint name :
HTTP Port : 80
Watch-list:
Enabled : no
Webauth login-auth-bypass:
```

```
Device# show parameter-map type webauth name global
Parameter Map Name : global
Type : webauth
Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window : Enabled
Webauth success-window : Enabled
Consent Email : Disabled
Sleeping-Client : Disabled
Webauth login-auth-bypass:
```

External Web Authentication (EWA)

Configuring EWA with Single WebAuth Server Address and Default Ports (80/443) (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication login** **Example:** `Device(config)# aaa authentication login WEBAUTH local`	Defines the authentication method at login.
Step 3	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth ISE-Ext-Webauth_IP`	Creates the parameter map. The *parameter-map-name* must not exceed 99 characters.
Step 4	**type webauth** **Example:** `Device(config-params-parameter-map)# type webauth`	Configures the webauth type parameter.
Step 5	**redirect for-login** *URL-String* **Example:** `Device(config-params-parameter-map)# redirect for-login https://192.168.0.98:443/portal/PortalSetup.action?portal=[illegible]`	Configures the URL string for redirect during login.
Step 6	**redirect portal ipv4** *ip-address* **Example:** `Device(config-params-parameter-map)# redirect portal ipv4 192.168.0.98`	Configures the external portal IPv4 address.
Step 7	**exit** **Example:** `Device(config-params-parameter-map)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 8	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan EWLC3-GUEST 3 EWLC3-GUEST`	Configures a WLAN.
Step 9	**no security ft adaptive** **Example:** `Device(config-wlan)# no security ft adaptive`	Disables adaptive 11r.
Step 10	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 11	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 12	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 13	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 14	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for WLAN.
Step 15	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list WEBAUTH`	Enables authentication list for dot1x security.
Step 16	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map ISE-Ext-Webauth_IP`	Configures the parameter map. **Note** If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

	Command or Action	Purpose
Step 17	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring EWA with Multiple Web Servers and/or Ports Different than Default (80/443)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended preauth_ISE_Ext_WA`	Defines an extended IPv4 access list using a name, and enters access-list configuration mode.
Step 3	*access-list-number* **permit tcp any host** *external_web_server_ip_address1* **eq** *port-number* **Example:** `Device(config)# 10 permit tcp any host 192.168.0.98 eq 8443`	Permits access from any host to the external web server port number 8443.
Step 4	*access-list-number* **permit tcp any host** *external_web_server_ip_address2* **eq** *port-number* **Example:** `Device(config)# 10 permit tcp any host 192.168.0.99 eq 8443`	Permits access from any host to the external web server port number 8443.
Step 5	*access-list-number* **permit udp any any eq domain** **Example:** `Device(config)# 20 permit udp any any eq domain`	Permits DNS UDP traffic.
Step 6	*access-list-number* **permit udp any any eq bootpc** **Example:** `Device(config)# 30 permit udp any any eq bootpc`	Permits DHCP traffic.

	Command or Action	Purpose
Step 7	*access-list-number* **permit udp any any eq bootps** **Example:** `Device(config)# 40 permit udp any any eq bootps`	Permits DHCP traffic.
Step 8	*access-list-number* **permit tcp host** *external_web_server_ip_address1* **eq** *port_number* **any** **Example:** `Device(config)# 50 permit tcp host 192.168.0.98 eq 8443 any`	Permits the access from the external web server port 8443 to any host.
Step 9	*access-list-number* **permit tcp host** *external_web_server_ip_address2* **eq** *port_number* **any** **Example:** `Device(config)# 50 permit tcp host 192.168.0.99 eq 8443 any`	Permits the access from the external web server port 8443 to any host.
Step 10	*access-list-number* **permit tcp any any eq domain** **Example:** `Device(config)# 60 permit tcp any any eq domain`	Permits the DNS TCP traffic.
Step 11	*access-list-number* **deny ip any any** **Example:** `Device(config)# 70 deny ip any any`	Denies all the other traffic.
Step 12	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan EWLC3-GUEST 3 EWLC3-GUEST`	Creates the WLAN.
Step 13	**ip access-group web** *name* **Example:** `Device(config-wlan)# ip access-group web preauth_ISE_Ext_WA`	Configures the IPv4 WLAN web ACL. The variable *name* specifies the user-defined IPv4 ACL name.
Step 14	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Wired Guest EWA with Multiple Web Servers and/or Ports Different than Default (80/443)

Before you begin

You cannot assign a manual ACL to a wired guest LAN configuration. The workaround is to use the bypass ACL in the global parameter map.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended BYPASS_ACL`	Defines an extended IPv4 access list using a name, and enters access-list configuration mode.
Step 3	*access-list-number* **deny ip any host** *hostname* **Example:** `Device(config)# 10 deny ip any host 192.168.0.45`	Allows the traffic to switch centrally.
Step 4	*access-list-number* **deny ip any host** *hostname* **Example:** `Device(config)# 20 deny ip any host 4.0.0.1`	Allows the traffic to switch centrally.
Step 5	**parameter-map type webauth global** **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 6	**webauth-bypass-intercept** *name* **Example:** `Device(config-params-parameter-map)# webauth-bypass-intercept BYPASS_ACL`	Creates a WebAuth bypass intercept using the ACL name. **Note** You cannot apply a manual ACL to the wired guest profile and configure an external web authentication with multiple IP addresses or different ports. The workaround is to use the bypass ACL for wired guest profile.
Step 7	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-params-parameter-map)# end`	

Authentication for Sleeping Clients

Information About Authenticating Sleeping Clients

Clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which sleeping clients should be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can also configure this duration on WebAuth parameter map that is mapped to a WLAN. Note that the sleeping client timer comes into effect due to instances such as idle timeout, session timeout, disabling of the WLAN, and the AP being nonoperational.

This feature is supported in the following FlexConnect scenario: local switching and central authentication.

Caution If the MAC address of a client that goes to sleep mode is spoofed, the fake device such as a laptop can be authenticated.

Mobility Scenarios

Following are some guidelines in a mobility scenario:

- L2 roaming in the same subnet is supported.
- Anchor sleeping timer is applicable.
- The sleeping client information is shared between multiple autoanchors when a sleeping client moves from one anchor to another.

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two controller s in a mobility group. A client that is associated with one controller goes to sleep and then wakes up and gets associated with the other controller .
- Suppose there are three controller s in a mobility group. A client that is associated with the second controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third controller .
- A client sleeps, wakes up and gets associated with the same or different export foreign controller that is anchored to the export anchor.

Restrictions on Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security.
- You can configure the sleeping clients only on a per WebAuth parameter-map basis.

- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.

Configuring Authentication for Sleeping Clients (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

Step 3 Select **Sleeping Client Status** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Authentication for Sleeping Clients (CLI)

Procedure

	Command or Action	Purpose
Step 1	**[no] parameter-map type webauth** {*parameter-map-name* | **global**} **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 2	**sleeping-client** [**timeout** *time*] **Example:** `Device(config-params-parameter-map)# sleeping-client timeout 100`	Configures the sleeping client timeout to 100 minutes. Valid range is between 10 minutes and 43200 minutes. **Note** If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.
Step 3	**end**	Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 4	(Optional) **show wireless client sleeping-client** **Example:** `Device# show wireless client sleeping-client`	Shows the MAC address of the clients and the time remaining in their respective sessions.
Step 5	(Optional) **clear wireless client sleeping-client** [**mac-address** *mac-addr*] **Example:** `Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001`	• **clear wireless client sleeping-client**—Deletes all sleeping client entries from the sleeping client cache. • **clear wireless client sleeping-client mac-address** *mac-addr*—Deletes the specific MAC entry from the sleeping client cache.

Sleeping Clients with Multiple Authentications

Mobility Support for Sleeping Clients

From Release 17.1.1 onwards, mobility support for guest and nonguest sleeping clients.

Supported Combinations of Multiple Authentications

Multiple authentication feature supports sleeping clients configured in the WLAN profile.

The following table outlines the supported combination of multiple authentications:

Table 72: Supported Combinations of Multiple Authentications

Layer 2	Layer 3	Supported
MAB	LWA	Yes
MAB Failure	LWA	Yes
Dot1x	LWA	Yes
PSK	LWA	Yes

Configuring Sleeping Clients with Multiple Authentications

Configuring WLAN for Dot1x and Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name* - Profile name of the configured WLAN. • *wlan-id* - Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - SSID, which can contain up to 32 alphanumeric characters.
Step 3	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 4	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Configures web authentication.
Step 5	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Maps the parameter map. **Note**: If the parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**no shutdown** **Example:**	Enables WLAN.

	Command or Action	Purpose
	`Device(config-wlan)# no shutdown`	

Configuring a WLAN for MAC Authentication Bypass and Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name* - Profile name of the configured WLAN. • *wlan-id* - Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - SSID, which can contain up to 32 alphanumeric characters.
Step 3	**mac-filtering** *list-name* **Example:** `Device(config-wlan)# mac-filtering cat-radius`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables the WPA2 cipher. **aes**—Excryption type that specifies WPA/AES support.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Maps the parameter map. **Note**: If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**no shutdown** **Example:**	Enables WLAN.

	Command or Action	Purpose
	`Device(config-wlan)# no shutdown`	

Configuring a WLAN for Local Web Authentication and MAC Filtering

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name* - Profile name of the configured WLAN. • *wlan-id* - Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - SSID, which can contain up to 32 alphanumeric characters.
Step 3	**mac-filtering** *list-name* **Example:** `Device(config-wlan)# mac-filtering cat-radius`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security Authenticated Key Management (AKM) for dot1x.
Step 5	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables the WPA2 cipher. **aes**: Excryption type that specifies WPA/AES support.
Step 6	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure wlan-id`	Configures the fallback policy with MAC filtering and web authentication.
Step 7	**security web-auth parameter-map** *parameter-map-name*	Maps the parameter map.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth parameter-map global`	**Note**: If the parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables WLAN.

Configuring a PSK + LWA in a WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name* - Profile name of the configured WLAN. • *wlan-id* - Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - SSID, which can contain up to 32 alphanumeric characters.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for a WLAN.
Step 5	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables the WPA2 cipher. **aes**: Excryption type that specifies WPA/AES support.
Step 6	**security wpa psk set-key ascii** *ascii/hex key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 1234567`	Configures the preshared key on a WLAN.

	Command or Action	Purpose
Step 7	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK support.
Step 8	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables the authentication list for dot1x security.
Step 9	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Maps the parameter map. **Note**: If the parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

Configuring a Sleeping Client

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** {*parameter-map-name* | **global**} **Example:** `Device(config)# parameter-map type webauth MAP-2`	Creates a parameter map and enters *parameter-map-name* configuration mode. The specific configuration commands supported for a **global** parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the *parameter-map-name* argument.
Step 3	**sleeping client** [**timeout** *time*] **Example:** `Device(config-params-parameter-map)# sleeping-client timeout 60`	Configures the sleeping client timeout, in minutes. The available range for the *time* argument is from 10 to 43200. **Note**: If you do not use the **timeout** keyword, the sleeping client is configured with the default timeout value of 720 minutes.

Verifying a Sleeping Client Configuration

To verify a sleeping client configuration, use the following command:

```
Device# show wireless client sleeping-client
Total number of sleeping-client entries: 1

MAC Address                    Remaining time (mm:ss)
------------------------------------------------------------
2477.031b.aa18                 59:56
```

Multi Authentication Combination with 802.1X Authentication and Local Web Authentication

Feature History for Multiauthentication Combination of 802.1X and Local Web Authentication

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 73: Feature History for Multiauthentication Combination of 802.1X and Local Web Authentication

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.11.1	Multiauthentication Combination of 802.1X and Local Web Authentication	This feature supports the merging of applied policies during multiauthentication of 802.1X or MAC authentication bypass (MAB) and local web authentication (LWA).

Information About Multiauthentication Combination with 802.1X Authentication and Local Web Authentication

In a wireless setup, for example, in a university, clients authenticate through 802.1X authentication. Because the 802.1X (dot1X) authentication process is secure and does not require user intervention, the end-users are unaware of the network that their devices are connected to. This could lead to serious concerns if they connect to the university's wireless network and post inappropriate content or access restricted content.

To avoid this situation, web authentication (webauth) and 802.1X authentication are configured in the network. End-user consent is used as a part of webauth to inform users that they are connected to the university's Wi-Fi network.

When the end-users accept the credentials for consent, AAA policies are not applied. The AAA policies that were applied earlier are deleted, resulting in a VLAN change and client disconnection.

A new command is introduced in Cisco IOS XE Dublin 17.11.1 to fix this issue. When you run the **consent activation-mode merge** command, the policy that is applied through consent is merged with the policy applied

for 802.1X or MAC Authentication Bypass (MAB) authentication, thereby allowing clients to access the network. This command is available in parameter-map mode, which is configured with **type consent** command.

Limitations for Multi Authentication Combination of 802.1X and Local Web Authentication

The following are the limitations for multiauthentication combination of 802.1X authentication and LWA:

- It is not possible to configure this feature on the controller GUI.
- SNMP is not supported.
- When the **consent activation-mode merge** command is not configured on the webauth parameter map, the default activation mode is Replace. This means that the user profile for consent replaces all the user profile policies that were previously applied.

Enabling the Multiauthentication Combination of 802.1X Authentication and Local Web Authentication (CLI)

Before you begin

Ensure that you have working knowledge of multiauthentication concepts, LWA (consent), and AAA override.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enter global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth parameter-map1`	Configures the webauth type parameter. Enters the parameter map configuration mode.
Step 3	**type consent** **Example:** `Device(config-params-parameter-map)# type consent`	Configures the type as **consent**.
Step 4	**[no] consent** {**activation-mode merge** | **email**} **Example:** `Device(config-params-parameter-map)# consent activation-mode merge`	Enables policy activation mode and merges the previous policy. Run the **no** form of this command to disable the feature.

Verifying Multiauthentication Combination with 802.1X Authentication and Local Web Authentication

To verify the multiauthentication combination with 802.1X authentication and LWA, run the following command:

```
Device# show parameter-map type webauth lwa-consent
Parameter Map Name               : lwa_consent
  Banner Title                   : Consent Title
  Banner Text                    : Please accept the consent
  Type                           : consent
  Auth-proxy Init State time     : 300 sec
  Webauth max-http connection    : 200
  Webauth logout-window          : Enabled
  Webauth success-window         : Enabled
  Consent Email                  : Disabled
  Activation Mode                : Merge
  Sleeping-Client                : Disabled
  Webauth login-auth-bypass:
```



CHAPTER 90

Central Web Authentication

- Information About Central Web Authentication, on page 985
- How to Configure ISE, on page 986
- How to Configure Central Web Authentication on the Controller, on page 988
- Authentication for Sleeping Clients, on page 996
- Sleeping Clients with Multiple Authentications, on page 998

Information About Central Web Authentication

Central web authentication offers the possibility to have a central device that acts as a web portal (in this example, the ISE). The major difference compared to the usual local web authentication is that it is shifted to Layer 2 along with MAC filtering or dot1x authentication. The concept also differs in that the radius server (ISE in this example) returns special attributes that indicate to the switch that a web redirection must occur. This solution eliminates any delay to start the web authentication.

The following are the different types of web authentication methods:

- Local Web Authentication (LWA): Configured as Layer 3 security on the controller, the web authentication page and the pre-authentication ACL are locally configured on the controller. The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server.
- External Web Authentication (EWA): Configured as Layer 3 security on the controller, the controller intercepts htttp(s) traffic and redirects the client to the login page hosted on the external web server. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is configured statically on the controller.
- Central Web Authentication (CWA): Configured mostly as Layer 2 security on the controller, the redirection URL and the pre-authentication ACL reside on ISE and are pushed during layer 2 authentication to the controller. The controller redirects all web traffic from the client to the ISE login page. ISE validates the credentials entered by the client through HTTPS and authenticates the user.

Globally, if the MAC address of the client station is not known by the radius server (but other criteria can also be used), the server returns the redirection attributes, and the controller authorizes the station (using the MAC filtering) but places an access list to redirect the web traffic to the portal.

Once the user logs into the guest portal, it is possible to re-authenticate the client so that a new Layer 2 MAC filtering occurs using the Change of Authorization (CoA). This way, the ISE remembers that it was a webauth user and pushes the necessary authorization attributes to the controller for accessing the network.

Note

- In Central Web Authentication (CWA) with dual VLAN posture scenario, Cisco AireOS and IOS-XE controller performs 2 and 3 EAPOL handshakes respectively. If a client is stuck in a quarantine VLAN because of any break in EAPOL handshake due to client or network issue, you need to analyze the client or network issue.
- However, you can manually disconnect or reconnect the client to come out of the quarantine loop (or) click the Scan Again on AnyConnect (Or) enable posture lease (Or) use the ISE posture sync feature.
- If the controller has no switch virtual interface (SVI) in the client subnet or VLAN, the controller has to use any of the other SVIs and send traffic as defined in the routing table. This means that the traffic is sent to another gateway in the core of the network; this traffic then reaches the client subnet. Firewalls typically block traffic from and to the same switch, as seen in this scenario, so redirection might not work properly. Workarounds are to allow this behavior on the firewall.

Prerequisites for Central Web Authentication

- Cisco Identity Services Engine (ISE)

How to Configure ISE

To configure ISE, proceed as follows:

1. Create an authorization profile.
2. Create an authentication rule.
3. Create an authorization rule.

Creating an Authorization Profile

Procedure

Step 1 Click **Policy**, and click **Policy Elements**.

Step 2 Click **Results**.

Step 3 Expand **Authorization**, and click **Authorization Profiles**.

Step 4 Click **Add** to create a new authorization profile for central webauth.

Step 5 In the **Name** field, enter a name for the profile. For example, CentralWebauth.

Step 6 Choose **ACCESS_ACCEPT** from the Access Type drop-down list.

Step 7 Check the **Web Redirection (CWA, MDM, NSP, CPP)** check box, and choose **Centralized Web Auth** from the drop-down list.

Step 8 In the **ACL** field, enter the name of the ACL that defines the traffic to be redirected. For example, redirect.

Step 9 In the **Value** field, choose the default or customized values.

The Value attribute defines whether the ISE sees the default or a custom web portal that the ISE admin created.

Step 10 Click **Save**.

Creating an Authentication Rule

Follow the procedure given below to use the authentication profile and create the authentication rule:

Procedure

Step 1 In the **Policy** > **Authentication** page, click **Authentication**.

Step 2 Enter a name for your authentication rule. For example, MAB.

Step 3 In the If condition field, select the plus (+) icon.

Step 4 Choose **Compound condition**, and choose **Wireless_MAB**.

Step 5 Click the arrow located next to **and ...** in order to expand the rule further.

Step 6 Click the + icon in the Identity Source field, and choose **Internal endpoints**.

Step 7 Choose **Continue** from the 'If user not found' drop-down list.

This option allows a device to be authenticated even if its MAC address is not known.

Step 8 Click **Save**.

Creating an Authorization Rule

You can configure many rules in the authorization policy. The *MAC not known* rule is configured in this section:

Procedure

Step 1 Click **Policy** > **Authorization**.

Step 2 In the Rule Name field, enter a name. For example: *Mac not known*.

Step 3 In the Conditions field, click the plus (+) icon.

Step 4 Choose **Compound Conditions**, and choose **Wireless_MAB**.

Step 5 From the settings icon, select **Add Attribute/Value** from the options.

Step 6 In the Description field, choose **Network Access** > **AuthenticationStatus** as the attribute from the drop-down list.

Step 7 Choose the **Equals** operator.

Step 8 From the right-hand field, choose **UnknownUser**.

Step 9 In the Permissions field, choose the authorization profile name that you had created earlier.

The ISE continues even though the user (or MAC) is not known.

Unknown users are now presented with the Login page. However, once they enter their credentials, they are presented again with an authentication request on the ISE; therefore, another rule must be configured with a condition that is met if the user is a guest user. For example, if UseridentityGroup Equals Guest is used then it is assumed that all guests belong to this group.

Step 10 In the Conditions field, click the plus (+) icon.

Step 11 Choose **Compound Conditions**, and choose to create a new condition.

The new rule must come before the *MAC not known* rule.

Step 12 From the settings icon, select **Add Attribute/Value** from the options.

Step 13 In the Description field, choose **Network Access** > **UseCase** as the attribute from the drop-down list.

Step 14 Choose the **Equals** operator.

Step 15 From the right-hand field, choose **GuestFlow**.

Step 16 In the Permissions field, click the plus (+) icon to select a result for your rule.

You can choose **Standard** > **PermitAccess** option or create a custom profile to return the attributes that you like.

When the user is authorized on the login page, the ISE triggers a COA that results in the restart of Layer 2 authentication. When the user is identified as a guest user, the user is authorized.

How to Configure Central Web Authentication on the Controller

To configure central web authentication on the controller, proceed as follows:

1. Configure WLAN.
2. Configure policy profile.
3. Configure redirect ACL.
4. Configure AAA for central web authentication.
5. Configure redirect ACL in Flex profile.

Configuring WLAN (GUI)

Before you begin

You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 In the **WLANs** window, click the name of the **WLAN** or click **Add** to create a new one.

Step 3 In the **Add/Edit WLAN** window that is displayed, click the **General** tab to configure the following parameters.

- In the **Profile Name** field, enter or edit the name of the profile.
- In the **SSID** field, enter or edit the SSID name.

  The SSID name can be alphanumeric, and up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number. The valid range is between 1 and 512.
- From the **Radio Policy** drop-down list, choose the **802.11** radio band.
- Using the **Broadcast SSID** toggle button, change the status to either **Enabled** or **Disabled** .
- Using the **Status** toggle button, change the status to either **Enabled** or **Disabled** .

Step 4 Click the **Security** tab, and then **Layer 2** tab to configure the following parameters:

- From the **Layer 2 Security Mode** drop-down list, choose **None**. .This setting disables Layer 2 security.
- Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.
- Check the **Over the DS** check box to enable Fast Transition over a distributed system.
- Choose OWE, Opportunistic Wireless Encryption (OWE) provides data confidentiality with encryption over the air between an AP radio and a wireless client. OWE Transition Mode is meant to provide a sort of backwards compatibility.
- Choose Fast Transition, 802.11r which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition.
- Check the check box to enable MAC filtering in the WLAN.
- Check the **Lobby Admin Access** check box to enable Lobby Admin access.

Step 5 Click **Save & Apply to Device**.

Configuring WLAN (CLI)

Configure WLAN using commands.

Note You need to enable MAC filtering for Layer 2 authentication to download the redirect URL and ACL.

After completing the WLAN configuration, if the changes are not pushed to all the APs, the following syslog message appears:

2021/01/06 16:20:00.597927186 {wncd_x_R0-4}{1}: [wlanmgr-db] [20583]: UUID: 0, ra: 0, TID: 0 (note): Unable to push WLAN config changes to all APs, cleanup required for WlanId: 2, profile: wlan1 state: Delete pending

If the above mentioned syslog message appears for more than six minutes, reload the controller.

If the controller does not reload and still the syslog message appears, then collect the archive logs, wncd core file, and raise a case by clicking the following link: Support Case Manager.

Procedure

	Command or Action	Purpose
Step 1	**wlan wlan-name wlan-id SSID-name** **Example:** `Device(config)# wlan wlanProfileName 1 ngwcSSID`	Enters the WLAN configuration sub-mode. **wlan-name** is the name of the configured WLAN. **wlan-id** is the wireless LAN identifier. The range is 1 to 512. **SSID-name** is the SSID name which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan wlan-name** command.
Step 2	**mac-filtering** [*name*] **Example:** `Device(config-wlan)# mac-filtering name`	Enables MAC filtering on a WLAN. **Note** While configuring mac-filtering the default authentication list is considered, if the authentication list is not configured earlier.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disable WPA security.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 5	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Example

```
Device# config terminal
Device(config)# wlan wlanProfileName 1 ngwcSSID
Device(config-wlan)# mac-filtering default
Device(config-wlan)# no security wpa
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

Configuring Policy Profile (CLI)

Configure Policy Profile using commands.

Note You need a AAA override to apply policies coming from the AAA or ISE servers. When a redirect URL and redirect ACL is received from the ISE server, NAC is used to trigger the Central Web Authentication (CWA).

Both NAC and AAA override must be available in the policy profile to which the client is being associated.

The default policy profile is associated to an AP, if the AP is not associated to any other policy profiles.

Procedure

	Command or Action	Purpose
Step 1	**wireless profile policy default-policy-profile** **Example:** `Device(config)# wireless profile policy default-policy-profile`	Sets the policy profile.
Step 2	**vlan `vlan-id`** **Example:** `Device(config-wireless-policy)# vlan 41`	Maps the VLAN to a policy profile. If vlan-id is not specified, the default native vlan 1 is applied. The valid range for vlan-id is 1 to 4096. Management VLAN is applied if no VLAN is configured on the policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA or ISE servers.
Step 4	**nac** **Example:** `Device(config-wireless-policy)# nac`	Configures Network Access Control in the policy profile. NAC is used to trigger the Central Web Authentication (CWA).
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the WLAN.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Example

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# vlan 41
Device(config-wireless-policy)# aaa-override
Device(config-wireless-policy)# nac
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end
```

Configuring a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click **Add**.

Step 3 In the **Add Policy Profile** window, in General Tab, enter a name and description for the policy profile.

Step 4 To enable the policy profile, set **Status** as Enabled.

Step 5 Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.

Step 6 (Optional) In the **CTS Policy** section, choose the appropriate status for the following:

- Inline Tagging—a transport mechanism using which a controller embedded wireless controller or access point understands the source SGT.
- SGACL Enforcement

Step 7 Specify a default **SGT**. The valid range is from 2 to 65519.

Step 8 In the WLAN Switching Policy section, choose the following, as required:

- Central Switching
- Central Authentication
- Central DHCP
- Central Association Enable
- Flex NAT/PAT

Step 9 Click **Save & Apply to Device**.

Creating Redirect ACL

The redirect ACL is a punt ACL that needs to be predefined on the controller (or the AP in case of FlexConnect local switching): the AAA server returns the name of the ACL and not its definition. The redirect ACL defines traffic (matching "deny"statements, as it denies redirection for it) that will be allowed through on the data plane and traffic (matching "permit" statements) that will be sent to the control plane towards the CPU for further processing (that is, the web interception and redirection in this case). The ACL has implicit (that is, the invisible) statements allowing DHCP and DNS traffic towards all IPs, just like it is the case with LWA. It also ends with a statement that a security ACL implicit deny.

Procedure

	Command or Action	Purpose
Step 1	**ip access-list extended redirect** **Example:** `Device(config)# ip access-list extended redirect`	The HTTP and HTTPS browsing does not work without authentication (per the other ACL) as ISE is configured to use a redirect ACL (named **`redirect`**).
Step 2	**deny ip any host `ISE-IP-add`** **Example:** `Device(config)# deny ip any host 123.123.134.112`	Allows traffic to ISE and all other traffic is blocked.
Step 3	**deny ip host `ISE-IP-add` any** **Example:** `Device(config)# deny ip host 123.123.134.112 any`	Allows traffic to ISE and all other traffic is blocked. **Note** This ACL is applicable for both local and flex mode.

Step 4	**permit TCP any any eq `web address/port-number`**
	Example:
	In case of HTTP:
	`Device(config)# permit TCP any any eq www`
	`Device(config)# permit TCP any any eq 80`
	Example:
	In case of HTTPS:
	`Device(config)# permit TCP any any eq 443`
		Redirects all HTTP or HTTPS access to the ISE login page. port-number 80 is used for HTTP and port-number 443 is used for HTTPS.
		For the ACE to allow traffic to ISE, ISE should be configured above the HTTP/HTTPS ACE.

Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring AAA for Central Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures the Change of Authorization (CoA) on the controller.
Step 2	**client `ISE-IP-add` server-key `radius-shared-secret`** **Example:** `Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET`	Specifies a RADIUS client and the RADIUS key to be shared between a device and a RADIUS client. **ISE-IP-add** is the IP address of the RADIUS client. **server-key** is the radius client server-key. **radius-shared-secret** covers the following: • **0**—Specifies unencrypted key. • **6**—Specifies encrypted key. • **7**—Specifies HIDDEN key. • **Word**—Unencrypted (cleartext) server key. The RADIUS shared secret should not exceed 240 characters while configuring WSMA data in GUI. **Note** All these steps work only if the AAA configuration is in place. See the *Configuring AAA Authentication* for details.

Example

```
Device# config terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET
Device(config-locsvr-da-radius)# end
```

Configuring Redirect ACL in Flex Profile (GUI)

The redirect ACL definition must be sent to the access point in the FlexConnect profile. For this, the redirect ACL associated with an AP must be configured in the FlexConnect profile where the client is hosted. If an

access point is not configured with any of the FlexConnect profiles, the default FlexConnect profile is associated with it.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 On the **Flex Profile** page, click the name of the FlexConnect profile or click **Add** to create a new FlexConnect profile.

Step 3 In the **Add/Edit Flex Profile** window that is displayed, click the **Policy ACL** tab.

Step 4 Click **Add** to map an ACL to the FlexConnect profile.

Step 5 Choose the ACL name, enable central web authentication, and specify the preauthentication URL filter.

Step 6 Click **Save**.

Step 7 Click **Update & Apply to Device**.

Configuring Redirect ACL in Flex Profile (CLI)

The redirect ACL definition must be sent to the access point in the Flex profile. For this, the redirect ACL associated to an AP must be configured in the Flex profile where the client is being hosted. If an access point is not configured with any of the Flex profiles, the default Flex profile is associated with it.

Note When the ACL is pushed down to the APs, the permission must change from **deny** to **permit** or vice-versa. This change does not occur if the ACL contains an object group, causing the ACL not to be fully translated, which may cause the redirection to fail.

Procedure

	Command or Action	Purpose
Step 1	**wireless profile flex default-flex-profile** **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy. The default flex profile name is **`default-flex-profile`**.
Step 2	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy acl1`	Configures ACL policy.
Step 3	**central-webauth** **Example:** `Device(config-wireless-flex-profile-acl)# central-webauth`	Configures central web authentication.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-wireless-flex-profile-acl)# end`	Returns to privileged EXEC mode.

Troubleshooting Central Web Authentication

Init-State timer running out

Problem Issue: The client devices are deauthenticated by the controller if users fail to enter their credentials in a limited time interval. The clients are deauthenticated after three times the time configured for the init-state timeout in the controller.

Problem Explanation: This is the expected functionality as the init-state timeout is not directly applicable for central web authentication; instead, it is the reap timer's value which is three times the init-state time plus five seconds (3*init-state timeout + 5) that determines the time interval in seconds for client deauthentication. For example, if you have configured the init-state timeout as 10 seconds, then the client devices are deuathenticated if users fail to enter their credentials after 35 seconds; that is (3*10 + 5) = 35 seconds.

Authentication for Sleeping Clients

Information About Authenticating Sleeping Clients

Clients with guest access that have had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which sleeping clients should be remembered for before reauthentication becomes necessary. The valid range is 10 minutes to 43200 minutes, with the default being 720 minutes. You can also configure this duration on WebAuth parameter map that is mapped to a WLAN. Note that the sleeping client timer comes into effect due to instances such as idle timeout, session timeout, disabling of the WLAN, and the AP being nonoperational.

This feature is supported in the following FlexConnect scenario: local switching and central authentication.



Caution If the MAC address of a client that goes to sleep mode is spoofed, the fake device such as a laptop can be authenticated.

Mobility Scenarios

Following are some guidelines in a mobility scenario:

- L2 roaming in the same subnet is supported.
- Anchor sleeping timer is applicable.
- The sleeping client information is shared between multiple autoanchors when a sleeping client moves from one anchor to another.

A sleeping client does not require reauthentication in the following scenarios:

- Suppose there are two controller s in a mobility group. A client that is associated with one controller goes to sleep and then wakes up and gets associated with the other controller .
- Suppose there are three controller s in a mobility group. A client that is associated with the second controller that is anchored to the first controller goes to sleep, wakes up, and gets associated with the third controller .
- A client sleeps, wakes up and gets associated with the same or different export foreign controller that is anchored to the export anchor.

Restrictions on Authenticating Sleeping Clients

- The sleep client feature works only for WLAN configured with WebAuth security.
- You can configure the sleeping clients only on a per WebAuth parameter-map basis.
- The authentication of sleeping clients feature is supported only on WLANs that have Layer 3 security enabled.
- With Layer 3 security, the Authentication, Passthrough, and On MAC Filter failure web policies are supported. The Conditional Web Redirect and Splash Page Web Redirect web policies are not supported.
- The central web authentication of sleeping clients is not supported.
- The authentication of sleeping clients feature is not supported on guest LANs and remote LANs.
- A guest access sleeping client that has a local user policy is not supported. In this case, the WLAN-specific timer is applied.

Configuring Authentication for Sleeping Clients (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

Step 3 Select **Sleeping Client Status** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Authentication for Sleeping Clients (CLI)

Procedure

	Command or Action	Purpose
Step 1	**[no] parameter-map type webauth** {*parameter-map-name* | **global**} **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 2	**sleeping-client** [**timeout** *time*] **Example:** `Device(config-params-parameter-map)# sleeping-client timeout 100`	Configures the sleeping client timeout to 100 minutes. Valid range is between 10 minutes and 43200 minutes. **Note** If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.
Step 3	**end**	Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.
Step 4	(Optional) **show wireless client sleeping-client** **Example:** `Device# show wireless client sleeping-client`	Shows the MAC address of the clients and the time remaining in their respective sessions.
Step 5	(Optional) **clear wireless client sleeping-client** [**mac-address** *mac-addr*] **Example:** `Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001`	• **clear wireless client sleeping-client**—Deletes all sleeping client entries from the sleeping client cache. • **clear wireless client sleeping-client mac-address** *mac-addr*—Deletes the specific MAC entry from the sleeping client cache.

Sleeping Clients with Multiple Authentications

Mobility Support for Sleeping Clients

From Release 17.1.1 onwards, mobility support for guest and nonguest sleeping clients.

Supported Combinations of Multiple Authentications

Multiple authentication feature supports sleeping clients configured in the WLAN profile.

The following table outlines the supported combination of multiple authentications:

Table 74: Supported Combinations of Multiple Authentications

Layer 2	Layer 3	Supported
MAB	LWA	Yes
MAB Failure	LWA	Yes
Dot1x	LWA	Yes
PSK	LWA	Yes

Configuring Sleeping Clients with Multiple Authentications

Configuring WLAN for Dot1x and Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name* - Profile name of the configured WLAN. • *wlan-id* - Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - SSID, which can contain up to 32 alphanumeric characters.
Step 3	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 4	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Configures web authentication.

	Command or Action	Purpose
Step 5	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Maps the parameter map. **Note**: If the parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables WLAN.

Configuring a WLAN for MAC Authentication Bypass and Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name* - Profile name of the configured WLAN. • *wlan-id* - Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - SSID, which can contain up to 32 alphanumeric characters.
Step 3	**mac-filtering** *list-name* **Example:** `Device(config-wlan)# mac-filtering cat-radius`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:**	Disables security AKM for dot1x.

	Command or Action	Purpose
	`Device(config-wlan)# no security wpa akm dot1x`	
Step 5	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables the WPA2 cipher. **aes**—Excryption type that specifies WPA/AES support.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Maps the parameter map. **Note**: If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables WLAN.

Configuring a WLAN for Local Web Authentication and MAC Filtering

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name* - Profile name of the configured WLAN. • *wlan-id* - Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - SSID, which can contain up to 32 alphanumeric characters.
Step 3	**mac-filtering** *list-name* **Example:** `Device(config-wlan)# mac-filtering cat-radius`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:**	Disables security Authenticated Key Management (AKM) for dot1x.

	Command or Action	Purpose
	`Device(config-wlan)#  no security wpa akm dot1x`	
Step 5	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables the WPA2 cipher. **aes**: Excryption type that specifies WPA/AES support.
Step 6	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure wlan-id`	Configures the fallback policy with MAC filtering and web authentication.
Step 7	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Maps the parameter map. **Note**: If the parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables WLAN.

Configuring a PSK + LWA in a WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name* - Profile name of the configured WLAN. • *wlan-id* - Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - SSID, which can contain up to 32 alphanumeric characters.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)#  no security wpa akm dot1x`	Disables security AKM for dot1x.

	Command or Action	Purpose
Step 4	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for a WLAN.
Step 5	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables the WPA2 cipher. **aes**: Excryption type that specifies WPA/AES support.
Step 6	**security wpa psk set-key ascii** *ascii/hex key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 1234567`	Configures the preshared key on a WLAN.
Step 7	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK support.
Step 8	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables the authentication list for dot1x security.
Step 9	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Maps the parameter map. **Note**: If the parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

Configuring a Sleeping Client

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** {*parameter-map-name* | **global**} **Example:**	Creates a parameter map and enters *parameter-map-name* configuration mode.

	Command or Action	Purpose
	`Device(config)# parameter-map type webauth MAP-2`	The specific configuration commands supported for a **global** parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the *parameter-map-name* argument.
Step 3	**sleeping client** [**timeout** *time*] **Example:** `Device(config-params-parameter-map)# sleeping-client timeout 60`	Configures the sleeping client timeout, in minutes. The available range for the *time* argument is from 10 to 43200. **Note**: If you do not use the **timeout** keyword, the sleeping client is configured with the default timeout value of 720 minutes.

Verifying a Sleeping Client Configuration

To verify a sleeping client configuration, use the following command:

```
Device# show wireless client sleeping-client
Total number of sleeping-client entries: 1

MAC Address                    Remaining time (mm:ss)
------------------------------------------------------
2477.031b.aa18                 59:56
```



CHAPTER 91

Private Shared Key

- Information About Private Preshared Key, on page 1005
- Configuring a PSK in a WLAN (CLI), on page 1006
- Configuring a PSK in a WLAN (GUI), on page 1007
- Applying a Policy Profile to a WLAN (GUI), on page 1008
- Applying a Policy Profile to a WLAN (CLI), on page 1008
- Verifying a Private PSK, on page 1009

Information About Private Preshared Key

With the advent of Internet of Things (IoT), the number of devices that connect to the internet has increased multifold. Not all of these devices support the 802.1x supplicant and need an alternate mechanism to connect to the internet. One of the security mechanisms, WPA-PSK, could be considered as an alternative. With the current configuration, the PSK is the same for all the clients that connect to the same WLAN. In certain deployments, such as educational institutions, this results in the key being shared to unauthorized users leading to security breach. This necessitates the need to provision unique PSKs for different clients on a large scale.

Identity PSKs are unique PSKs created for individuals or groups of users on the same SSID. No complex configuration is required for the clients. It provides the same simplicity of PSK, making it ideal for IoT, Bring your own device (BYOD), and guest deployments.

Identity PSKs are supported on most devices, in which 802.1X is not, enabling stronger security for IoT. It is possible to easily revoke access, for a single device or individual without affecting everyone else. Thousands of keys can easily be managed and distributed through the AAA server.

Note Special characters, such as '<' and '>' are supported in SSID Preshared key.

Note PSK supports whitespace in passwords (before or after or in-between) within double quotes only; single quotes for whitespaces are not supported.

IPSK Solution

During client authentication, the AAA server authorizes the client MAC address and sends the passphrase (if configured) as part of the Cisco-AV pair list. The Cisco Wireless Controller (WLC) receives this as part of the RADIUS response and processes this further for the computation of PSKs.

When a client sends an association request to the SSID broadcast by the corresponding access point, the controller forms the RADIUS request packet with the particular mac address of the client and relays to the RADIUS server.

The RADIUS server performs the authentication and checks whether the client is allowed or not and sends either ACCESS-ACCEPT or ACCESS-REJECT as response to the WLC.

To support Identity PSKs, in addition to sending the authentication response, the authentication server also provides the AV pair passphrase for this specific client. This is used for the computation of the PMK.

The RADIUS server might also provide additional parameters, such as username, VLAN, Quality of Service (QoS), and so on, in the response, that is specific to this client. For multiple devices owned by a single user, the passphrase can remain the same.

Note When the PSK length is less than 15 characters in Federal Information Processing Standard (FIPS), the controller allows the WLAN configuration but displays the following error message on the console:

"AP is allowed to join but corresponding WLAN will not be pushed to the access point"

Configuring a PSK in a WLAN (CLI)

Follow the procedure given below to configure a PSK in a WLAN:

Before you begin

- Security should be configured for a pre-shared key (PSK) in a WLAN.
- If there is no override from the AAA server, the value on the corresponding WLAN is considered for authentication.
- In Federal Information Processing Standard (FIPS) and common criteria mode, ensure that the PSK WLAN has a minimum of 15 ASCII characters, else APs won't join the controller.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan test-profile 4 abc`	Configures the WLAN and SSID.

	Command or Action	Purpose
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures the security type PSK.
Step 5	**security wpa akm psk set-key** *ascii/hex key* **Example:** `Device(config-wlan)# security wpa akm psk set-key asci 0`	Configures the PSK authenticated key management (AKM) shared key. **Note** You must set the **psk set-key** before configuring AKM PSK.
Step 6	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK support.
Step 7	**security wpa wpa2 mpsk** **Example:** `Device(config-wlan)# security wpa wpa2 mpsk`	Configures multi-preshared key (MPSK) support. **Note** AKM PSK should be enabled for MPSK to work.
Step 8	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test1`	Specifies MAC filtering in a WLAN.

Configuring a PSK in a WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **Wireless Networks** page, click **Security** tab.

Step 3 In the **Layer 2** window that is displayed, go to the **WPA Parameters** section.

Step 4 From the **Auth Key Mgmt** drop-down, select the PSK format and type.

Step 5 Enter the Pre-Shared Key in hexadecimal characters.

- If you selected the PSK format as HEX, the key length must be exactly 64 characters.
- If you selected the PSK format as ASCII, the key length must be in the range of 8-63 characters.

Note that once you have configured the key, these details are not visible even if you click on the eye icon next to the preshared key box, due to security reasons.

Step 6 Click **Save & Apply to Device**.

Applying a Policy Profile to a WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.
Step 2 On the**Manage Tags** page, click **Policy** tab.
Step 3 Click **Add** to view the **Add Policy Tag** window.
Step 4 Enter a name and description for the policy tag.
Step 5 Click **Add** to map WLAN and policy.
Step 6 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.
Step 7 Click **Save & Apply to Device**.

Applying a Policy Profile to a WLAN (CLI)

Follow the procedure given below to a apply policy profile to a WLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-iot`	Configures the default policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA server or ISE the Cisco Identify Services Engine (ISE) server.

Verifying a Private PSK

Use the following **show** commands to verify the configuration of a WLAN and a client:

```
Device# show wlan id 2


WLAN Profile Name     : test_ppsk
===============================================
Identifier                                      : 2
Network Name (SSID)                             : test_ppsk
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 0
Number of Active Clients                        : 0
Exclusionlist Timeout                           : 60
CHD per WLAN                                    : Enabled
Interface                                       : default
Multicast Interface                             : Unconfigured
WMM                                             : Allowed
WifiDirect                                      : Invalid
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Diagnostics Channel Capability            : Disabled
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : test1
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Enabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            PMF dot1x                           : Disabled
            PMF PSK                             : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Disabled
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Disabled
```

```
        PMF Association Comeback Timeout       : 1
        PMF SA Query Time                      : 200
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : Disabled
    Webauth Parameter Map                      : Disabled
    Tkip MIC Countermeasure Hold-down Timer    : 60
Call Snooping                                  : Disabled
Passive Client                                 : Disabled
Non Cisco WGB                                  : Disabled
Band Select                                    : Disabled
Load Balancing                                 : Disabled
Multicast Buffer                               : Disabled
Multicast Buffer Size                          : 0
IP Source Guard                                : Disabled
Assisted-Roaming
    Neighbor List                              : Disabled
    Prediction List                            : Disabled
    Dual Band Support                          : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                 : Disabled
    BSS Max Idle                               : Disabled
        Protected Mode                         : Disabled
    Traffic Filtering Service                  : Disabled
    BSS Transition                             : Enabled
        Disassociation Imminent                : Disabled
            Optimised Roaming Timer            : 40
            Timer                              : 200
    WNM Sleep Mode                             : Disabled
802.11ac MU-MIMO                               : Disabled
```

```
Device# show wireless client mac-address a886.adb2.05f9 detail
```

```
Client MAC Address : a886.adb2.05f9
Client IPv4 Address : 9.9.58.246
Client Username : A8-86-AD-B2-05-F9
AP MAC Address : c025.5c55.e400
AP Name: saurabh-3600
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id : 6
Wireless LAN Name: SSS_PPSK
BSSID : c025.5c55.e40f
Connected For : 280 seconds
Protocol : 802.11n - 5 GHz
Channel : 60
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 320 sec (Remaining time: 40 sec)
Input Policy Name  :
Input Policy State : None
Input Policy Source : None
Output Policy Name  :
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
```

```
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Current Rate : m22
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 09/27/2017 16:32:25 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 280 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : PSK
AAA override passphrase: Yes
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 58
Access VLAN : 58
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_90000005
  IIF ID           : 0x90000005
  Device Type      : Apple-Device
  Protocol Map     : 0x000001
  Authorized       : TRUE
  Session timeout  : 320
  Common Session ID: 1F3809090000005DC30088EA
  Acct Session ID  : 0x00000000
  Auth Method Status List
        Method : MAB
                SM State        : TERMINATE
                Authen Status   : Success
  Local Policies:
        Service Template : wlan_svc_default-policy-profile (priority 254)
                Absolute-Timer   : 320
                VLAN             : 58
  Server Policies:
  Resultant Policies:
                VLAN             : 58
                Absolute-Timer   : 320
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Central
FlexConnect Central Association : No
```

```
Client Statistics:
  Number of Bytes Received : 59795
  Number of Bytes Sent : 21404
  Number of Packets Received : 518
  Number of Packets Sent : 274
  Number of EAP Id Request Msg Timeouts :
  Number of EAP Request Msg Timeouts :
  Number of EAP Key Msg Timeouts :
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -32 dBm
  Signal to Noise Ratio : 58 dB
Fabric status : Disabled
```



CHAPTER 92

Multi-Preshared Key

- Information About Multi-Preshared Key, on page 1013
- Restrictions on Multi-PSK, on page 1014
- Configuring Multi-Preshared Key (GUI), on page 1014
- Configuring Multi-Preshared Key (CLI), on page 1017
- Verifying Multi-PSK Configurations, on page 1018

Information About Multi-Preshared Key

Multi-PSK feature supports multiple PSKs simultaneously on a single SSID. You can use any of the configured PSKs to join the network. This is different from the Identity PSK (iPSK), wherein unique PSKs are created for individuals or groups of users on the same SSID.

From 16.10 onwards, each SSID supports five PSKs, which can be extended

In a traditional PSK, all the clients joining the network use the same password as shown in the below figure.

Figure 30: Traditional PSK



But with multi-PSK, client can use any of the configured pre-shared keys to connect to the network as shown in the below figure.

Figure 31: Multi-PSK



In Multi-PSK, two passwords are configured (deadbeef and beefdead) for the same SSID. In this scenario, clients can connect to the network using either of the passwords.

Restrictions on Multi-PSK

- Central authentication is supported in local, flex, and fabric modes only.
- In central authentication flex mode, the standalone AP allows client join with the highest priority PSK (*priority 0* key). New clients that do not use the highest priority PSK are rejected during the standalone mode.
- Multi-PSK does not support local authentication.
- Multi-PSK is different from iPSK. In iPSK, the PSK password comes from ISE authorization policy, so MAB is required. MPSK uses a pool of passwords locally configured in WLAN, so ISE is not used.

Configuring Multi-Preshared Key (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **Wireless Networks** page, click the name of the WLAN.

Step 3 In the **Edit WLAN** window, click the **Security** tab.

Step 4 In the **Layer2** tab, choose the **Layer2 Security Mode** from the following options:

- None: No Layer 2 security
- 802.1X: WEP 802.1X data encryption type

- WPA + WPA2: Wi-Fi Protected Access
- Static WEP: Static WEP encryption parameters
- Static WEP+802.1X: Both Static WEP and 802.1X parameters

Parameters	Description
802.1X	
WEP Key Size	Choose the key size. The available values are *None*, *40 bits*, and *104 bits*.
WPA + WPA2	
Protected Management Frame	Choose from the following options: • Disabled • Optional • Required
WPA Policy	Check the check box to enable WPA policy.
WPA Encryption	Choose the WPA encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.
WPA2 Policy	Check the check box to enable WPA2 policy.
WPA2 Encryption	Choose the WPA2 encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.
Auth Key Mgmt	Choose the rekeying mechanism from the following options: • 802.1X • FT + 802.1X • PSK: You must specify the PSK format and a preshared key • Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value • 802.1X + Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value • FT + 802.1X + Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value

Parameters	Description
Static WEP	
Key Size	Choose the key size from the following options: • 40 bits • 104 bits
Key Index	Choose a key index from 1 to 4. One unique WEP key index can be applied to each WLAN. As there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer2 encryption.
Key Format	Choose the encryption key format as either ASCII or HEX.
Encryption Key	Enter an encryption key that is 13 characters long.
Static WEP + 802.1X	
Key Size	Choose the key size from the following options: • 40 bits • 104 bits
Key Index	Choose a key index from 1 to 4. One unique WEP key index can be applied to each WLAN. As there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer2 encryption.
Key Format	Choose the encryption key format as either ASCII or HEX.
Encryption Key	Enter an encryption key that is 13 characters long.
WEP Key Size	Choose from the following options: • None • 40 bits • 104 bits

Step 5 Click **Save & Apply to Device**.

Configuring Multi-Preshared Key (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan mywlan 1 SSID_name`	Configures WLAN and SSID.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK.
Step 5	**security wpa wpa2 mpsk** **Example:** `Device(config-wlan)# security wpa wpa2 mpsk`	Configures multi-PSK.
Step 6	**priority** *priority_value* **set-key** {**ascii** [**0** | **8**] *pre-shared-key* | **hex** [**0** | **8**] *pre-shared-key*} **Example:** `Device(config-mpsk)# priority 0 set-key ascii 0 deadbeef`	Configures PSK priority and all its related passwords. The *priority_value* ranges from 0 to 4. **Note** You need to configure **priority 0** key for multi-PSK.
Step 7	**no shutdown** **Example:** `Device(config-mpsk)# no shutdown`	Enables WLAN.
Step 8	**exit** **Example:** `Device(config-wlan)# exit`	Exits WLAN configuration mode and returns to configuration mode.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Multi-PSK Configurations

To verify the configuration of a WLAN and a client, use the following command:

```
Device# show wlan id 8
WLAN Profile Name     : wlan_8
================================================
Identifier                                    : 8
Network Name (SSID)                           : ssid_8
Status                                        : Enabled
Broadcast SSID                                : Enabled
Universal AP Admin                            : Disabled
Max Associated Clients per WLAN               : 0
Max Associated Clients per AP per WLAN        : 0
Max Associated Clients per AP Radio per WLAN  : 200
Number of Active Clients                      : 0
CHD per WLAN                                  : Enabled
Multicast Interface                           : Unconfigured
WMM                                           : Allowed
WifiDirect                                    : Invalid
Channel Scan Defer Priority:
  Priority (default)                          : 5
  Priority (default)                          : 6
Scan Defer Time (msecs)                       : 100
Media Stream Multicast-direct                 : Disabled
CCX - AironetIe Support                       : Enabled
CCX - Diagnostics Channel Capability          : Disabled
Peer-to-Peer Blocking Action                  : Disabled
Radio Policy                                  : All
DTIM period for 802.11a radio                 : 1
DTIM period for 802.11b radio                 : 1
Local EAP Authentication                      : Disabled
Mac Filter Authorization list name            : Disabled
Mac Filter Override Authorization list name   : Disabled
Accounting list name                          :
802.1x authentication list name               : Disabled
802.1x authorization list name                : Disabled
Security
    802.11 Authentication                     : Open System
    Static WEP Keys                           : Disabled
    802.1X                                    : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)    : Enabled
        WPA (SSN IE)                          : Disabled
        WPA2 (RSN IE)                         : Enabled
            MPSK                              : Enabled
            AES Cipher                        : Enabled
            CCMP256 Cipher                    : Disabled
            GCMP128 Cipher                    : Disabled
            GCMP256 Cipher                    : Disabled
        WPA3 (WPA3 IE)                        : Disabled
        Auth Key Management
            802.1x                            : Disabled
            PSK                               : Enabled
```

```
            CCKM                                    : Disabled
            FT dot1x                                : Disabled
            FT PSK                                  : Disabled
            FT SAE                                  : Disabled
            PMF dot1x                               : Disabled
            PMF PSK                                 : Disabled
            SAE                                     : Disabled
            OWE                                     : Disabled
            SUITEB-1X                               : Disabled
            SUITEB192-1X                            : Disabled
    CCKM TSF Tolerance                              : 1000
    FT Support                                      : Adaptive
        FT Reassociation Timeout                    : 20
        FT Over-The-DS mode                         : Enabled
    PMF Support                                     : Disabled
        PMF Association Comeback Timeout            : 1
        PMF SA Query Time                           : 200
    Web Based Authentication                        : Disabled
    Conditional Web Redirect                        : Disabled
    Splash-Page Web Redirect                        : Disabled
    Webauth On-mac-filter Failure                   : Disabled
    Webauth Authentication List Name                : Disabled
    Webauth Authorization List Name                 : Disabled
    Webauth Parameter Map                           : Disabled
    Tkip MIC Countermeasure Hold-down Timer         : 60
Non Cisco WGB                                       : Disabled
Band Select                                         : Enabled
Load Balancing                                      : Disabled
Multicast Buffer                                    : Disabled
Multicast Buffer Size                               : 0
IP Source Guard                                     : Disabled
Assisted-Roaming
    Neighbor List                                   : Disabled
    Prediction List                                 : Disabled
    Dual Band Support                               : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                      : Disabled
    BSS Max Idle                                    : Disabled
        Protected Mode                              : Disabled
    Traffic Filtering Service                       : Disabled
    BSS Transition                                  : Enabled
        Disassociation Imminent                     : Disabled
            Optimised Roaming Timer                 : 40
            Timer                                   : 200
    WNM Sleep Mode                                  : Disabled
802.11ac MU-MIMO                                    : Disabled
802.11ax paramters
    OFDMA Downlink                                  : unknown
    OFDMA Uplink                                    : unknown
    MU-MIMO Downlink                                : unknown
    MU-MIMO Uplink                                  : unknown
    BSS Color                                       : unknown
    Partial BSS Color                               : unknown
    BSS Color Code                                  :
```

To view the WLAN details, use the following command:

```
Device# show run wlan
wlan wlan_8 8 ssid_8
 security wpa psk set-key ascii 0 deadbeef
 no security wpa akm dot1x
 security wpa akm psk
 security wpa wpa2 mpsk
  priority 0 set-key ascii 0 deadbeef
  priority 1 set-key ascii 0 deaddead
```

```
 priority 2 set-key ascii 0 d123d123
 priority 3 set-key hex 0 02345678901234567890123456789012345678901234567890123456789012345678901234

 priority 4 set-key hex 0 12345678901234567890123456789012345678901234567890123456789012345678901234

no shutdown
```



CHAPTER 93

Multiple Authentications for a Client

- Information About Multiple Authentications for a Client, on page 1021
- Configuring Multiple Authentications for a Client, on page 1023
- Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Pre-Shared Key (CLI), on page 1029
- Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with OWE (CLI), on page 1031
- Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Secure Agile Exchange (CLI), on page 1033
- Configuring 802.1x and Central Web Authentication on Controller (CLIs), on page 1034
- Configuring ISE for Central Web Authentication with Dot1x (GUI), on page 1041
- Verifying Multiple Authentication Configurations, on page 1043

Information About Multiple Authentications for a Client

Multiple Authentication feature is an extension of Layer 2 and Layer 3 security types supported for client join.

Note You can enable both L2 and L3 authentication for a given SSID.

Note The Multiple Authentication feature is applicable for regular clients only.

Information About Supported Combination of Authentications for a Client

The Multiple Authentications for a Client feature supports multiple combination of authentications for a given client configured in the WLAN profile.

The following table outlines the supported combination of authentications:

Layer 2	Layer 3	Supported
MAB	CWA	Yes

MAB	LWA	Yes
MAB + PSK	-	Yes
MAB + 802.1X	-	Yes
MAB Failure	LWA	Yes
802.1X	CWA	Yes
802.1X	LWA	Yes
PSK	-	Yes
PSK	LWA	Yes
PSK	CWA	Yes
iPSK	-	Yes
iPSK	CWA	Yes
iPSK + MAB	CWA	Yes
iPSK	LWA	No
MAB Failure + PSK	LWA	Yes
MAB Failure + PSK	CWA	No
MAB Failure + OWE	LWA	Yes
MAB Failure + SAE	LWA	Yes

From 16.10.1 onwards, 802.1X configurations on WLAN support web authentication configurations with WPA or WPA2 configuration.

The feature also supports the following AP modes:

- Local
- FlexConnect
- Fabric

Jumbo Frame Support for RADIUS Packets

This document describes how to configure IP Maximum Transmission Unit (MTU) size for RADIUS server. RADIUS packets will get fragmented based on IP MTU, if source interface is attached to RADIUS group. With the new design, the RADIUS packets get fragmented at interface IP MTU configured value.

Note Fragmentation size is fixed.

Combination of Authentications on MAC Failure Not Supported on a Client

The following table outlines the combination of authentications on MAC failure that are not supported on a given client:

Authentication Types	Foreign	Anchor	Supported
WPA3-OWE+LWA	Cisco AireOS	Cisco Catalyst 9800 Controller	No
WPA3-SAE+LWA	Cisco AireOS	Cisco Catalyst 9800 Controller	No

Configuring Multiple Authentications for a Client

Configuring WLAN for 802.1X and Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 Select the required WLAN from the list of WLANs displayed.
Step 3 Choose **Security** > **Layer2** tab.
Step 4 Select the security method from the **Layer 2 Security Mode** drop-down list.
Step 5 In the **Auth Key Mgmt**, check the **802.1x** check box.
Step 6 Check the **MAC Filtering** check box to enable the feature.
Step 7 After MAC Filtering is enabled, from the **Authorization List** drop-down list, choose an option.
Step 8 Choose **Security** > **Layer3** tab.
Step 9 Check the **Web Policy** check box to enable web authentication policy.
Step 10 From the **Web Auth Parameter Map** and the **Authentication List** drop-down lists, choose an option.
Step 11 Click **Update & Apply to Device**.

Configuring WLAN for 802.1X and Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name*	Enters WLAN configuration sub-mode.

	Command or Action	Purpose
	Example: `Device(config)# wlan wlan-test 3 ssid-test`	• *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 4	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication.
Step 5	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Maps the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Example

```
wlan wlan-test 3 ssid-test
 security dot1x authentication-list default
 security web-auth
 security web-auth authentication-list default
 security web-auth parameter-map WLAN1_MAP
 no shutdown
```

Configuring WLAN for Preshared Key (PSK) and Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Select the required WLAN.

Step 3 Choose **Security** > **Layer2** tab.

Step 4 Select the security method from the **Layer 2 Security Mode** drop-down list.

Step 5 In the Auth Key Mgmt, uncheck the **802.1x** check box.

Step 6 Check the **PSK** check box.

Step 7 Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.

Step 8 Choose **Security** > **Layer3** tab.

Step 9 Check the **Web Policy** checkbox to enable web authentication policy.

Step 10 Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.

Step 11 Click **Update & Apply to Device**.

Configuring WLAN for Preshared Key (PSK) and Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration sub-mode. • *profile-name*- Is the profile name of the configured WLAN. • *wlan-id* - Is the wireless LAN identifier. Range is from 1 to 512. • *SSID_Name* - Is the SSID which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.

	Command or Action	Purpose
Step 3	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK shared key.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures the PSK support.
Step 6	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for WLAN.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list webauth`	Enables authentication list for dot1x security.
Step 8	**security web-auth parameter-map** *parameter-map-name* **Example:** `(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

Example

```
wlan wlan-test 3 ssid-test
 security wpa psk set-key ascii 0 PASSWORD
 no security wpa akm dot1x
 security wpa akm psk
 security web-auth
 security web-auth authentication-list webauth
 security web-auth parameter-map WLAN1_MAP
```

Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication (GUI)

Procedure

Step 1	Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2	Select the required WLAN.
Step 3	Choose **Security** > **Layer2** tab.
Step 4	Select the security method from the **Layer 2 Security Mode** drop-down list.
Step 5	In the **Auth Key Mgmt**, uncheck the **802.1x** check box.
Step 6	Check the **PSK** check box.
Step 7	Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.
Step 8	Check the **MAC Filtering** check box to enable the feature.
Step 9	With MAC Filtering enabled, choose the Authorization List from the **Authorization List** drop-down list.
Step 10	Choose **Security** > **Layer3** tab.
Step 11	Check the **Web Policy** checkbox to enable web authentication policy.
Step 12	Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.
Step 13	Click **Update &Apply to Device**.

Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication

Configuring WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration sub-mode. • *profile-name* - Is the profile name of the configured WLAN. • *wlan-id* - Is the wireless LAN identifier. Range is from 1 to 512.

	Command or Action	Purpose
		• *SSID_Name* - Is the SSID which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK AKM shared key.
Step 5	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.

Example

```
wlan wlan-test 3 ssid-test
 no security wpa akm dot1x
 security wpa psk set-key ascii 0 PASSWORD
 mac-filtering test-auth-list
```

Applying Policy Profile to a WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-iot`	Configures the default policy profile.

	Command or Action	Purpose
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA or ISE servers.
Step 4	**nac** **Example:** `Device(config-wireless-policy)# nac`	Configures NAC in the policy profile.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Shutdown the WLAN.
Step 6	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Example

```
wireless profile policy policy-iot
 aaa-override
 nac
 no shutdown
```

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Pre-Shared Key (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512.

	Command or Action	Purpose
		• *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK AKM shared key.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK support.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name*	Configures the parameter map.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	**Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with OWE (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.

	Command or Action	Purpose
Step 5	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 6	**security wpa akm owe** **Example:** `Device(config-wlan)# security wpa akm owe`	Enables WPA3 OWE support.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Secure Agile Exchange (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 6	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 7	**security web-auth authentication-list** *authenticate-list-name*	Enables authentication list for dot1x security.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth authentication-list default`	
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring 802.1x and Central Web Authentication on Controller (CLIs)

Creating AAA Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.

Configuring AAA Server for External Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius-server attribute wireless authentication call-station-id ap-name-ssid** **Example:** `Device(config)# radius-server attribute wireless authentication call-station-id ap-name-ssid`	Configures a call station identifier sent in the RADIUS authentication messages.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server ISE2`	Sets the RADIUS server.
Step 4	**address ipv4** *radius-server-ip-address* **Example:** `Device(config-radius-server)# address ipv4 111.111.111.111`	Specifies the RADIUS server address.
Step 5	**timeout** *seconds* **Example:** `Device(config-radius-server)# timeout 10`	Specify the time-out value in seconds. The range is between 10 and 1000 seconds.
Step 6	**retransmit** *number-of-retries* **Example:** `Device(config-radius-server)# retransmit 10`	Specify the number of retries to the server. The range is between 0 and 100.
Step 7	**key** *key* **Example:** `Device(config-radius-server)# key cisco`	Specifies the authentication and encryption key used between the device and the key string RADIUS daemon running on the RADIUS server. *key* covers the following: • 0—Specifies unencrypted key. • 6—Specifies encrypted key. • 7—Specifies HIDDEN key. • Word—Unencrypted (cleartext) server key.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 9	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius ISE2`	Creates a RADIUS server-group identification.
Step 10	**server name** *server-name* **Example:** `Device(config)# server name ISE2`	Configures the server name.
Step 11	**radius-server deadtime** *time-in-minutes* **Example:** `Device(config)# radius-server deadtime 5`	Defines the time in minutes when a server marked as DEAD is held in that state. Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval. *time-in-mins*—Valid values range from 1 to 1440 minutes. Default value is zero. To return to the default value, use the **no radius-server deadtime** command. The **radius-server deadtime** command can be configured globally or per aaa group server level. You can use the **show aaa dead-criteria** or **show aaa servers** command to check for dead-server detection. If the default value is zero, deadtime is not configured.

Configuring AAA for Authentication

Before you begin

Configure the RADIUS server and AAA group server.

Procedure

	Command or Action	Purpose
Step 1	**aaa authentication login** **Example:** `Device# aaa authentication login ISE_GROUP group ISE2 local`	Defines the authentication method at login.
Step 2	**aaa authentication dot1x** **Example:** `Device(config)# aaa authentication network ISE_GROUP group ISE2 local`	Defines the authentication method at dot1x.

Configuring Accounting Identity List

Before you begin

Configure the RADIUS server and AAA group server.

Procedure

	Command or Action	Purpose
Step 1	**aaa accounting identity** *named-list* **start-stop group** *server-group-name* **Example:** `Device# aaa accounting identity ISE start-stop group ISE2`	Enables accounting to send a start-record accounting notice when a client is authorized and a stop-record at the end. **Note** You can also use the default list instead of the named list.

Configuring AAA for Central Web Authentication

Before you begin

Configure the RADIUS server and AAA group server.

Procedure

	Command or Action	Purpose
Step 1	**aaa server radius dynamic-author** **Example:** `Device# aaa server radius dynamic-author`	Configures the Change of Authorization (CoA) on the controller.
Step 2	**client** *client-ip-addr* **server-key** *key* **Example:**	Configures a server key for a RADIUS client.

	Command or Action	Purpose
	`Device(config-locsvr-da-radius)# client 111.111.111.111 server-key ciscokey`	

Defining an Access Control List for Radius Server

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended redirect** **Example:** `Device(config)# ip access-list extended redirect`	The HTTP and HTTPS browsing does not work without authentication (per the other ACL) as ISE is configured to use a redirect ACL (named **redirect**).
Step 3	*sequence-number* **deny icmp any** **Example:** `Device(config-ext-nacl)# 10 deny icmp any`	Specifies packets to reject according to the sequence number. **Note** You must have the DHCP, DNS, and ISE servers in the reject sequences. Refer to Configuration Example to Define an Access Control List for Radius Server, wherein the *111.111.111.111* refers to the IP address of the ISE server.
Step 4	**permit TCP any any eq** *web-address* **Example:** `Device(config-ext-nacl)# permit TCP any any eq www`	Redirects all HTTP or HTTPS access to the Cisco ISE login page.

Configuration Example to Define an Access Control List for Radius Server

This example shows how to define an access control list for RADIUS server:

```
Device# configure terminal
Device(config-ext-nacl) # 10 deny icmp any
Device(config-ext-nacl) # 20 deny udp any any eq bootps
Device(config-ext-nacl) # 30 deny udp any any eq bootpc
Device(config-ext-nacl) # 40 deny udp any any eq domain
Device(config-ext-nacl) # 50 deny tcp any host 111.111.111.111 eq 8443
Device(config-ext-nacl) # 55 deny tcp host 111.111.111.111 eq 8443 any
Device(config-ext-nacl) # 40 deny udp any any eq domain
Device(config-ext-nacl) # end
```

Configuring WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Device(config)# wlan wlan30`	Enters WLAN configuration mode.
Step 3	**security dot1x authentication-list ISE_GROUP** **Example:** `Device(config-wlan)# security dot1x authentication-list ISE_GROUP`	Configures 802.1X for a WLAN.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy wireless-profile1`	Configures policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the AAA or Cisco Identify Services Engine (ISE) server.
Step 4	**accounting-list** *list-name* **Example:**	Sets the accounting list for IEEE 802.1x.

	Command or Action	Purpose
	`Device(config-wireless-policy)# accounting-list ISE`	
Step 5	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures DHCP parameters for WLAN.
Step 6	**nac** **Example:** `Device(config-wireless-policy)# nac`	Configures Network Access Control (NAC) in the policy profile. NAC is used to trigger the Central Web Authentication (CWA).
Step 7	**vlan 25** **Example:** `Device(config-wireless-policy)# vlan 25`	Configures guest VLAN profile.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.

Mapping WLAN and Policy Profile to Policy Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy xx-xre-policy-tag`	Configures policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan wlan30 policy wireless-profile1`	Maps a policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.

Configuring ISE for Central Web Authentication with Dot1x (GUI)

Defining Guest Portal

Before you begin

Define the guest portal or use the default guest portal.

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).
Step 2 Choose **Work Centers** > **Guest Access** > **Portals & Components**.
Step 3 Click **Guest Portal**.

Defining Authorization Profile for a Client

Before you begin

You can define the authorization profile to use guest portal and other additional parameters as per the requirement. Authorization profile redirects the client to the authentication portal. In the latest Cisco ISE version, Cisco_Webauth authorization results exist already, and you can edit the same to modify the redirection ACL name to match the configuration in the controller.

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).
Step 2 Choose **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**.
Step 3 Click **Add** to create your own custom or edit the Cisco_Webauth default result.

Defining Authentication Rule

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).
Step 2 Choose **Policy** > **Policy Sets** and click on the appropriate policy set.
Step 3 Expand **Authentication** policy.

Step 4 Expand **Options** and choose an appropriate **User ID**.

Defining Authorization Rule

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).

Step 2 Choose **Policy** > **Policy Sets** > **Authorization Policy**.

Step 3 Create a rule that matches the condition for 802.1x with a specific SSID (using Radius-Called-Station-ID).

Note You get to view the CWA redirect attribute.

Step 4 Choose the already created authorization profile.

Step 5 From the **Result/Profile** column, choose the already created authorization profile.

Step 6 Click **Save**.

Note The following image depicts the working configuration sample for your reference.

Figure 32: Working Configuration Sample



Creating Rules to Match Guest Flow Condition

Before you begin

You must create a second rule that matches the guest flow condition and returns to network access details once the user completes authentication in the portal.

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).

Step 2 Choose **Policy** > **Policy Sets** > **Authorization Policy**.

Step 3 Create a rule that matches the condition for 802.1x with, Network Access-UseCase EQUALS Guest, and a specific SSID (using Radius-Called-Station-ID).

Note You get to view the Permit Access.

Step 4 From the **Result/Profile** column, choose the already created authorization profile.

Step 5 Choose the default or customized Permit Access.

Step 6 Click **Save**.

Verifying Multiple Authentication Configurations

Layer 2 Authentication

After L2 authentication (Dot1x) is complete, the client is moved to *Webauth Pending* state.

To verify the client state after L2 authentication, use the following commands:

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------------

58ef.68b6.aa60 ewlc1_ap_1   3  Webauth Pending    11n(5)        Dot1x  Local
Number of Excluded Clients: 0
```

```
Device# show wireless client mac-address <mac_address> detail

Auth Method Status List

Method: Dot1x
Webauth State: Init
Webauth Method: Webauth
Local Policies:
Service Template: IP-Adm-V6-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V6-Int-ACL-global
Service Template: IP-Adm-V4-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V4-Int-ACL-global
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50
```

```
Device# show platform software wireless-client chassis active R0

        ID  MAC Address      WLAN  Client     State
-----------------------------------------------------------------------------------------
  0xa0000003      58ef.68b6.aa60    3             L3          Authentication
```

```
Device# show platform software wireless-client chassis active F0

    ID     MAC Address   WLAN  Client     State  AOM ID    Status
-----------------------------------------------------------------------------------------------------
0xa0000003    58ef.68b6.aa60    3           L3          Authentication.         730.
Done
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO    LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN

Mobility State Abbreviations:
```

```
UK - UNKNOWN       IN - INIT
LC - LOCAL               AN - ANCHOR
FR - FOREIGN          MT - MTE
IV - INVALID


EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
------------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary
Vlan   DP IDX         MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
------------------------------------------------------------------------------------
0X49   0xa0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

Layer 3 Authentication

Once L3 authentication is successful, the client is moved to *Run* state.

To verify the client state after L3 authentication, use the following commands:

```
Device# show wireless client summary

Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------------------------

58ef.68b6.aa60   ewlc1_ap_1  3     Run    11n(5)   Web Auth      Local
Number of Excluded Clients: 0
```

```
Device# show wireless client mac-address 58ef.68b6.aa60 detail

Auth Method Status List

Method: Web Auth
Webauth State: Authz
Webauth Method: Webauth
Local Policies:
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

Server Policies:

Resultant Policies:
VLAN: 50
Absolute-Timer: 1800
```

```
Device# show platform software wireless-client chassis active R0

ID          MAC Address     WLAN    Client State
-----------------------------------------------
0xa0000001 58ef.68b6.aa60    3          Run
```

```
Device# show platform software wireless-client chassis active f0

ID         MAC Address       WLAN    Client State   AOM ID.  Status
-------------------------------------------------------------------
0xa0000001 58ef.68b6.aa60.   3          Run         11633    Done
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary
```

```
Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO      LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL         AN - ANCHOR
FR - FOREIGN       MT - MTE
IV - INVALID
EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address   VLAN  CT  MCVL AS MS E   WLAN     POA
------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60  50   RG   0   RN LC N wlan-test 0x90000003

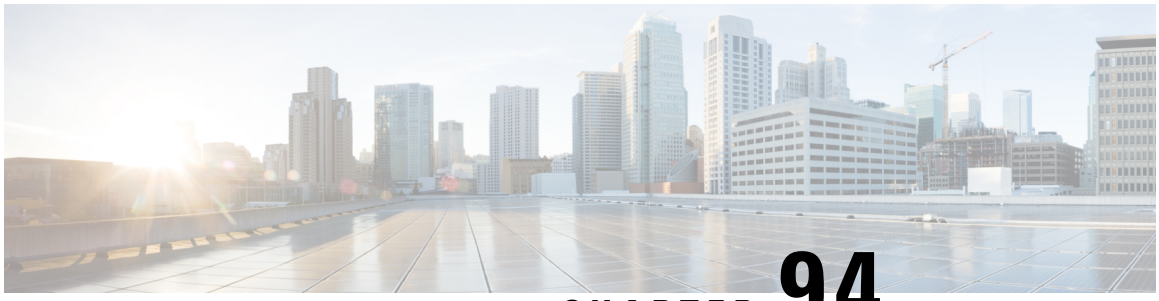
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary

Vlan   pal_if_hd1        mac           Input Uidb     Output Uidb
-----------------------------------------------------------------
50     0xa0000003    58ef.68b6.aa60     95929            95927
```

Verifying PSK+Webauth Configuration

```
Device# show wlan summary

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 12:08:32.941 CEST Tue Oct 6 2020


Number of WLANs: 1

ID Profile Name SSID Status Security
-------------------------------------------------------------------------------------------------------------------------------

23 Gladius1-PSKWEBAUTH Gladius1-PSKWEBAUTH UP [WPA2][PSK][AES],[Web Auth]
```



CHAPTER 94

Wi-Fi Protected Access 3

- Simultaneous Authentication of Equals, on page 1047
- Opportunistic Wireless Encryption, on page 1048
- Hash-to-Element (H2E), on page 1048
- YANG (RPC model), on page 1049
- Transition Disable, on page 1051
- WPA3 SAE iPSK, on page 1051
- Configuring SAE (WPA3+WPA2 Mixed Mode), on page 1051
- Configuring WPA3 Enterprise (GUI), on page 1053
- Configuring WPA3 Enterprise, on page 1053
- Configuring the WPA3 OWE, on page 1055
- Configuring WPA3 OWE Transition Mode (GUI), on page 1056
- Configuring WPA3 OWE Transition Mode, on page 1056
- Configuring WPA3 SAE (GUI), on page 1058
- Configuring WPA3 SAE, on page 1058
- Configuring WPA3 SAE iPSK (CLI), on page 1060
- Configuring WPA3 SAE H2E (GUI), on page 1063
- Configuring WPA3 SAE H2E, on page 1063
- Configuring WPA3 WLAN for Transition Disable, on page 1065
- Configuring Anti-Clogging and SAE Retransmission (GUI), on page 1066
- Configuring Anti-Clogging and SAE Retransmission, on page 1066
- Verifying WPA3 SAE and OWE, on page 1067
- Verifying WPA3 SAE H2E Support in WLAN, on page 1071
- Verifying WPA3 Transition Disable in WLAN, on page 1076

Simultaneous Authentication of Equals

WPA3 is the latest version of Wi-Fi Protected Access (WPA), which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks.

WPA3 leverages Simultaneous Authentication of Equals (SAE) to provide stronger protections for users against password guessing attempts by third parties. SAE employs a discrete logarithm cryptography to perform an efficient exchange in a way that performs mutual authentication using a password that is probably resistant to an offline dictionary attack. An offline dictionary attack is where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

WPA3-Personal brings better protection to individual users by providing more robust password-based authentication making the brute-force dictionary attack much more difficult and time-consuming, while WPA3-Enterprise provides higher grade security protocols for sensitive data networks.

When the client connects to the access point, they perform an SAE exchange. If successful, they will each create a cryptographically strong key, from which the session key will be derived. Basically a client and access point goes into phases of commit and then confirm. Once there is a commitment, the client and access point can then go into the confirm states each time there is a session key to be generated. The method uses forward secrecy, where an intruder could crack a single key, but not all of the other keys.

Note Home SSIDs configured using OEAP GUI does not support WPA3 security in Cisco IOS-XE 17.6 and 17.7 releases.

Note Cisco Wave 2 APs do not support SAE. As a result, the AP clients are not able to connect to SAE SSID with these APs, as the clients fail to join back after receiving M3 from the APs.

The following are the Cisco Wave 2 APs that do not support SAE:

- Cisco Aironet 1815 Series APs (AP1815W, AP1815T, AP1815I, AP1815M)
- Cisco Aironet 1815T OfficeExtend APs
- Cisco Aironet 1800 Series APs (AP1800I, AP1800S)
- Cisco Aironet 1542 Series Outdoor APs (AP1542D, AP1542I)
- Cisco Aironet 1840 Series APs (AP1840I)

Opportunistic Wireless Encryption

Opportunistic Wireless Encryption (OWE) is an extension to IEEE 802.11 that provides encryption of the wireless medium. The purpose of OWE based authentication is avoid open unsecured wireless connectivity between the AP's and clients. The OWE uses the Diffie-Hellman algorithms based Cryptography to setup the wireless encryption. With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise secret with the 4-way handshake. The use of OWE enhances wireless network security for deployments where Open or shared PSK based networks are deployed.

Hash-to-Element (H2E)

Hash-to-Element (H2E) is a new SAE Password Element (PWE) method. In this method, the secret PWE used in the SAE protocol is generated from a password.

When a STA that supports H2E initiates SAE with an AP, it checks whether AP supports H2E. If yes, the AP uses the H2E to derive the PWE by using a newly defined Status Code value in the SAE Commit message.

If STA uses Hunting-and-Pecking, the entire SAE exchange remains unchanged.

While using the H2E, the PWE derivation is divided into the following components:

- Derivation of a secret intermediary element PT from the password. This can be performed offline when the password is initially configured on the device for each supported group.
- Derivation of the PWE from the stored PT. This depends on the negotiated group and MAC addresses of peers. This is performed in real-time during the SAE exchange.

Note

- 6-GHz supports only Hash-to-Element SAE PWE method.
- The H2E method also incorporates protection against the Group Downgrade man-in-the-middle attacks. During the SAE exchange, the peers exchange lists of rejected groups binded into the PMK derivation. Each peer compares the received list with the list of groups supported, any discrepancy detects a downgrade attack and terminates the authentication.

YANG (RPC model)

To create an RPC for SAE Password Element (PWE) mode, use the following RPC model:

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:0a77124f-c563-469d-bd21-cc625a9691cc">
<nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
<wlan-cfg-entries>
<wlan-cfg-entry>
<profile-name>test</profile-name>
<wlan-id>2</wlan-id>
<sae-pwe-mode>both-h2e-hnp</sae-pwe-mode>
</wlan-cfg-entry>
</wlan-cfg-entries>
</wlan-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>
```

To delete a 6-GHz radio policy and modify the SAE Password Element (PWE) mode, use the following RPC model:

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:2b8c4be6-492e-4488-b2cf-1f2a1e39fa8c"><nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
<wlan-cfg-entries>
<wlan-cfg-entry>
<profile-name>test</profile-name>
<wlan-id>2</wlan-id>
<wlan-radio-policies>
<wlan-radio-policy nc:operation="delete">
<band>dot11-6-ghz-band</band>
```

```
</wlan-radio-policy>
</wlan-radio-policies>
</wlan-cfg-entry>
</wlan-cfg-entries>
</wlan-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>

##
Received message from host
<?xml version="1.0" ?>
<rpc-reply message-id="urn:uuid:2b8c4be6-492e-4488-b2cf-1f2a1e39fa8c"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>
NETCONF rpc COMPLETE
NETCONF SEND rpc
Requesting 'Dispatch'
Sending:

#1268
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:e19a3309-2509-446f-9dbe-c46a6de433db"><nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
<wlan-cfg-entries>
<wlan-cfg-entry>
<profile-name>test</profile-name>
<wlan-id>2</wlan-id>
<wlan-radio-policies>
<wlan-radio-policy nc:operation="merge">
<band>dot11-5-ghz-band</band>
</wlan-radio-policy>
</wlan-radio-policies>
<sae-pwe-mode>hunting-and-pecking-only</sae-pwe-mode>
</wlan-cfg-entry>
</wlan-cfg-entries>
</wlan-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>

##
Received message from host
<?xml version="1.0" ?>
<rpc-reply message-id="urn:uuid:e19a3309-2509-446f-9dbe-c46a6de433db"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>
NETCONF rpc COMPLETE
```

Note The **delete** operation performs one action at a time due to the current infra limitation. That is, in YANG module, the **delete** operation on multiple nodes are not supported.

Transition Disable

Transition Disable is an indication from an AP to an STA. This feature disables few transition modes for subsequent connections to the APs network.

An STA implementation might enable certain transition modes in a network profile. For example, a WPA3-Personal STA might enable the WPA3-Personal transition mode in a network profile by default. This enables a PSK algorithm. However, you can use the Transition Disable indication to disable transition modes for that network on a STA.

Note The Transition Disable indication provides protection against downgrade attacks.

An AP that uses Transition Disable indication does not necessarily disable the corresponding transition modes on its own BSS. For example, the APs in WPA3-Personal network might use the Transition Disable indication to ensure that all STAs supporting WPA3-Personal are protected against the downgrade attack. However, the WPA3-Personal transition mode is enabled on the BSS for the legacy STAs to connect.

WPA3 SAE iPSK

A RADIUS server and Identity PSK (iPSK) create unique preshared keys for individuals or a group of users present in the same SSID. This kind of setup is useful in networks where end-client devices do not support 802.1X authentication. However, you will need a more secure and granular authentication. From a client perspective, the WLAN looks identical to the traditional PSK network. If one of the PSKs is compromised, only the affected individual or group needs to update their PSK. The rest of the devices connected to the WLAN remain unaffected.

The Simultaneous Authentication of Equals (SAE) H2E authentication mode uses a password token derived from the SAE authentication passphrase. You can configure the passphrase in the WLAN profile for client authentication during commit and confirm message exchanges.

From Cisco IOS-XE 17.9.2, the iPSK passphrase is supported for SAE H2E authentication in Local mode. The iPSK passphrase is configured in the client authorization policy in the RADIUS server. The passphrase pushes the policy to the controller during client MAB authentication.

Note The iPSK passphrase replaces the one in the WLAN profile to generate password token. If the iPSK passphrase is not configured in the authorization policy, the SAE H2E falls back to the passphrase in the WLAN profile.

Configuring SAE (WPA3+WPA2 Mixed Mode)

Follow the procedure given below to configure WPA3+WPA2 mixed mode for SAE.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 6	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Configures WPA2 cipher. **Note** You can check whether cipher is configured using **no security wpa wpa2 ciphers aes**command. If cipher is not reset, configure the cipher.
Step 7	**security wpa psk set-key ascii** *value preshared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 8	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support. **Note** If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.

	Command or Action	Purpose
Step 9	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 10	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Enables AKM PSK support.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 12	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 Enterprise (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Choose **WPA2+WPA3** in **Layer 2 Security Mode** drop-down list.

Step 5 Uncheck the **WPA2 Policy** and **802.1x** check boxes.Check the **WPA3 Policy** and **802.1x-SHA256** check boxes.

Step 6 Choose **Security** > **AAA** tab, choose the Authentication List from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Configuring WPA3 Enterprise

Follow the procedure given below to configure WPA3 enterprise.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wl-dot1x 4 wl-dot1x`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 5	**security wpa akm dot1x-sha256** **Example:** `Device(config-wlan)# security wpa akm dot1x-sha256`	Configures 802.1x support.
Step 6	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 7	**security dot1x authentication-list** *list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list ipv6_ircm_aaa_list`	Configures security authentication list for dot1x security.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode. **Note** A WLAN configured with WPA3 enterprise (SUITEB192-1X) is not supported on C9115/C9120 APs.

Configuring the WPA3 OWE

Follow the procedure given below to configure WPA3 OWE.

Before you begin

Configure PMF internally. The associated ciphers configuration can use the WPA2 ciphers.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 4	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Enables WPA2 ciphers for AES. **Note** The ciphers for WPA2 and WPA3 are common.
Step 8	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.

	Command or Action	Purpose
Step 9	**security wpa akm owe** **Example:** `Device(config-wlan)# security wpa akm owe`	Enables WPA3 OWE support.
Step 10	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 11	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 OWE Transition Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Choose **WPA2+WPA3** in **Layer 2 Security Mode** drop-down list.

Step 5 Uncheck the **WPA2 Policy**, **802.1x**, **Over the DS**, **FT + 802.1x** and **FT + PSK**check boxes.Check the **WPA3 Policy**, **AES** and **OWE** check boxes.

Step 6 Enter the **Transition Mode WLAN ID**.

Step 7 Click **Apply to Device**.

Configuring WPA3 OWE Transition Mode

Follow the procedure given below to configure the WPA3 OWE transition mode.

Note Policy validation is not done between open WLAN and OWE WLAN. The operator is expected to configure them appropriately.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Enables WPA2 ciphers for AES.
Step 8	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 9	**security wpa akm owe** **Example:** `Device(config-wlan)# security wpa akm owe`	Enables WPA3 OWE support.
Step 10	**security wpa transition-mode-wlan-id** *wlan-id* **Example:**	Configures the open or OWE transition mode WLAN ID.

	Command or Action	Purpose
	`Device(config-wlan)# security wpa transition-mode-wlan-id 1`	**Note** Validation is not performed on the transition mode WLAN. The operator is expected to configure it correctly with OWE WLAN having open WLAN identifier and the opposite way. You should configure OWE WLAN ID as transition mode WLAN in open WLAN. Similarly, open WLAN should be configured as transition mode WLAN in OWE WLAN configuration.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 12	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 SAE (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Choose **WPA2+WPA3** in **Layer 2 Security Mode** drop-down list.

Step 5 Uncheck the **WPAPolicy**, **802.1x**, **Over the DS**, **FT + 802.1x** and **FT + PSK**check boxes.Check the **WPA3 Policy**, **AES** and **PSK** check boxes. Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.

Step 6 Click **Apply to Device**.

Configuring WPA3 SAE

Follow the procedure given below to configure WPA3 SAE.

Before you begin

Configure PMF internally. The associated ciphers configuration can use the WPA2 ciphers.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Configures WPA2 cipher. **Note** You can check whether cipher is configured using **no security wpa wpa2 ciphers aes**command. If cipher is not reset, configure the cipher.
Step 8	**security wpa psk set-key ascii** *value preshared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 9	**security wpa wpa3**	Enables WPA3 support.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security wpa wpa3`	**Note** If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.
Step 10	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 12	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 SAE iPSK (CLI)

Configuring a WPA3 SAE iPSK WLAN Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wl-sae-ipsk 8 wl-sae-ipsk`	Enters the WLAN configuration sub-mode.
Step 3	**mac-filtering** *mac-filter-name* **Example:** `Device(config-wlan)# mac-filtering aaa_list`	Sets MAC filtering support in WLAN.
Step 4	**no security ft adaptive** **Example:**	Disables adaptive 802.11r.

	Command or Action	Purpose
	`Device(config-wlan)# no security ft adaptive`	
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**security wpa psk set-key** [*ascii/hex*] **0** [*key*] **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 123456789`	Configures the preshared key in WLAN. **Note** WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
Step 7	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for 802.1X.
Step 8	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 9	**security wpa akm sae pwe h2e** **Example:** `Device(config-wlan)# security wpa akm sae pwe h2e`	Enables AKM SAE PWE support (hash-to-element). **Note** This step is applicable to Hunting and Pecking (HnP) password element method as well.
Step 10	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 11	**security pmf mandatory** **Example:** `Device(config-wlan)# security pmf mandatory`	Makes clients negotiate Protected Management Frames (PMF) protection in WLAN.
Step 12	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring a Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy po-sae-ipsk`	Configures policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply to the policies coming from the AAA or Cisco Identity Services Engine (ISE) server.
Step 4	**vlan 166** **Example:** `Device(config-wireless-policy)# vlan 166`	Configures VLAN.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.

Configuring a Passphrase in a Client Authorization Policy in the RADIUS Server(GUI)

Procedure

Step 1 Log in to the Cisco Identity Services Engine (ISE).

Step 2 Click **Policy** and then click **Policy Elements**.

Step 3 Click **Results**.

Step 4 Expand **Authorization** and click **Authorization Profiles**.

Step 5 Click **Add** to create a new authorization profile for the URL filter.

Step 6 In the **Name** field, enter a name for the profile, for example, *po-sae-ipsk*.

Step 7 From the **Access Type** drop-down list, choose **ACCESS_ACCEPT**.

Step 8 From the **Termination-Action** drop-down list, choose **RADIUS-Request**.

Step 9 In the **Advanced Attributes Setting** section, from the drop-down list, choose **Cisco:cisco-av-pair**.

Step 10 Enter the following one by one and click (+) icon after each of them:

- `cisco-av-pair = psk-mode=ascii`
- `cisco-av-pair = psk=123123123`

Step 11 Verify the contents in the **Attributes Details** section and click **Save**.

Configuring WPA3 SAE H2E (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA2+WPA3** or **WPA3**.

Step 5 Uncheck the **WPAPolicy**, **802.1x**, **Over the DS**, **FT + 802.1x** and **FT + PSK** check boxes. Check the **WPA3 Policy**, **AES** and **PSK** check boxes. Enter the **Pre-Shared Key** and from the **PSK Format** drop-down list, choose the PSK Format and from the **PSK Type** drop-down list, choose the PSK Type.

Step 6 Check the **SAE** check box.

Note SAE is enabled only if the Fast Transition is disabled.

Step 7 From the **SAE Password Element** drop-down list, choose **Hash to Element Only** to configure the WPA3 SAE H2E.

Step 8 Click **Apply to Device**.

Configuring WPA3 SAE H2E

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.

	Command or Action	Purpose
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Configures WPA2 cipher. **Note** You can check whether cipher is configured using **no security wpa wpa2 ciphers aes** command. If cipher is not reset, configure the cipher.
Step 8	**security wpa psk set-key ascii** *value preshared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 9	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 10	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 11	**security wpa akm sae pwe** {**h2e** | **hnp** | **both-h2e-hnp**} **Example:** `Device(config-wlan)# security wpa akm sae pwe`	Enables AKM SAE PWE support. PWE supports the following options: • h2e—Hash-to-Element only; disables HnP.

	Command or Action	Purpose
		• hnp—Hunting and Pecking only; disables H2E. • Both-h2e-hnp—Both Hash-to-Element and Hunting and Pecking support (Is the default option).
Step 12	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 13	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 WLAN for Transition Disable

Before you begin

You can enable Transition Disable only when the **security wpa wpa3** is enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**transition-disable** **Example:** `Device(config-wlan)# transition-disable`	Enables Transition Disable support.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring Anti-Clogging and SAE Retransmission (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 Click **Add**.
Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.
Step 4 Enable or disable **Status** and **Broadcast SSID** toggle buttons.
Step 5 From the **Radio Policy** drop-down list, choose a policy.
Step 6 Choose **Security** > **Layer2** tab. Check the **SAE** check box.
Step 7 Enter the **Anti Clogging Threshold**, **Max Retries** and **Retransmit Timeout**.
Step 8 Click **Apply to Device**.

Configuring Anti-Clogging and SAE Retransmission

Follow the procedure given below to configure anti-clogging and SAE retransmission.

Note If the simultaneous SAE ongoing sessions are more than the configured anti-clogging threshold, then anti-clogging mechanism is triggered.

Before you begin

Ensure that SAE WLAN configuration is in place, as the steps given below are incremental in nature, in addition to the SAE WLAN configuration.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**shutdown** **Example:** `Device(config-wlan)# no shutdown`	Disables the WLAN.

	Command or Action	Purpose
Step 4	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables simultaneous authentication of equals as a security protocol.
Step 5	**security wpa akm sae anti-clogging-threshold** *threshold* **Example:** `Device(config-wlan)# security wpa akm sae anti-clogging-threshold 2000`	Configures threshold on the number of open sessions to trigger the anti-clogging procedure for new sessions.
Step 6	**security wpa akm sae max-retries** *retry-limit* **Example:** `Device(config-wlan)# security wpa akm sae max-retries 10`	Configures the maximum number of retransmissions.
Step 7	**security wpa akm sae retransmit-timeout** *retransmit-timeout-limit* **Example:** `Device(config-wlan)# security wpa akm sae retransmit-timeout 500`	Configures SAE message retransmission timeout value.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Verifying WPA3 SAE and OWE

To view the system level statistics for the client that has undergone successful SAE authentication, SAE authentication failures, SAE ongoing sessions, SAE commit and confirm message exchanges, use the following show command:

```
Device# show wireless stats client detail

Total Number of Clients : 0

client global statistics:
------------------------------------------------------------------------------
Total association requests received             : 0
Total association attempts                      : 0
Total FT/LocalAuth requests                     : 0
Total association failures                      : 0
Total association response accepts              : 0
Total association response rejects              : 0
Total association response errors               : 0
```

```
Total association failures due to blacklist      : 0
Total association drops due to multicast mac     : 0
Total association drops due to throttling        : 0
Total association drops due to unknown bssid     : 0
Total association drops due to parse failure     : 0
Total association drops due to other reasons     : 0
Total association requests wired clients         : 0
Total association drops wired clients            : 0
Total association success wired clients          : 0
Total peer association requests wired clients    : 0
Total peer association drops wired clients       : 0
Total peer association success wired clients     : 0
Total 11r ft authentication requests received    : 0
Total 11r ft authentication response success     : 0
Total 11r ft authentication response failure     : 0
Total 11r ft action requests received            : 0
Total 11r ft action response success             : 0
Total 11r ft action response failure             : 0
Total AID allocation failures                    : 0
Total AID free failures                          : 0
Total roam attempts                              : 0
  Total CCKM roam attempts                       : 0
  Total 11r roam attempts                        : 0
  Total 11i fast roam attempts                   : 0
  Total 11i slow roam attempts                   : 0
  Total other roam type attempts                 : 0
Total roam failures in dot11                     : 0

Total WPA3 SAE attempts                          : 0
Total WPA3 SAE successful authentications        : 0
Total WPA3 SAE authentication failures           : 0
  Total incomplete protocol failures             : 0
Total WPA3 SAE commit messages received          : 0
Total WPA3 SAE commit messages rejected          : 0
  Total unsupported group rejections             : 0
Total WPA3 SAE commit messages sent              : 0
Total WPA3 SAE confirm messages received         : 0
Total WPA3 SAE confirm messages rejected         : 0
  Total WPA3 SAE confirm messgae field mismatch  : 0
  Total WPA3 SAE confirm message invalid length  : 0
Total WPA3 SAE confirm messages sent             : 0
Total WPA3 SAE Open Sessions                     : 0
Total SAE Message drops due to throttling        : 0

Total Flexconnect local-auth roam attempts       : 0
  Total AP 11i fast roam attempts                : 0
  Total 11i slow roam attempts                   : 0

Total client state starts                        : 0
Total client state associated                    : 0
Total client state l2auth success                : 0
Total client state l2auth failures               : 0
Total blacklisted clients on dot1xauth failure   : 0
Total client state mab attempts                  : 0
Total client state mab failed                    : 0
Total client state ip learn attempts             : 0
Total client state ip learn failed               : 0
Total client state l3 auth attempts              : 0
Total client state l3 auth failed                : 0
Total client state session push attempts         : 0
Total client state session push failed           : 0
Total client state run                           : 0
Total client deleted                             : 0
```

To view the WLAN summary details, use the following command.

```
Device# show wlan summary

Number of WLANs: 3

ID   Profile Name                     SSID                             Status Security

-------------------------------------------------------------------------------------------------
1    wlan-demo                       ssid-demo                       DOWN   [WPA3][SAE][AES]

3    CR1_SSID_mab-ext-radius          CR1_SSID_mab-ext-radius          DOWN
[WPA2][802.1x][AES]

109  guest-wlan1                      docssid                          DOWN
[WPA2][802.1x][AES],[Web Auth]
```

To view the WLAN properties (WPA2 and WPA3 mode) based on the WLAN ID, use the following command.

```
Device# show wlan id 1

WLAN Profile Name     : wlan-demo
================================================
Identifier                                     : 1

!
!
!
Security
    802.11 Authentication                      : Open System
    Static WEP Keys                            : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)     : Enabled
        WPA (SSN IE)                           : Disabled
        WPA2 (RSN IE)                          : Disabled
        WPA3 (WPA3 IE)                         : Enabled
            AES Cipher                         : Enabled
            CCMP256 Cipher                     : Disabled
            GCMP128 Cipher                     : Disabled
            GCMP256 Cipher                     : Disabled
        Auth Key Management
            802.1x                             : Disabled
            PSK                                : Disabled
            CCKM                               : Disabled
            FT dot1x                           : Disabled
            FT PSK                             : Disabled
            Dot1x-SHA256                       : Disabled
            PSK-SHA256                         : Disabled
            SAE                                : Enabled
            OWE                                : Disabled
            SUITEB-1X                          : Disabled
            SUITEB192-1X                       : Disabled
    CCKM TSF Tolerance                         : 1000
    OSEN                                       : Disabled
    FT Support                                 : Adaptive
        FT Reassociation Timeout               : 20
        FT Over-The-DS mode                    : Enabled
    PMF Support                                : Required
        PMF Association Comeback Timeout       : 1
        PMF SA Query Time                      : 200
    Web Based Authentication                   : Disabled
```

```
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Webauth On-mac-filter Failure               : Disabled
    Webauth Authentication List Name            : Disabled
    Webauth Authorization List Name             : Disabled
    Webauth Parameter Map                       : Disabled
!
!
!
```

To view the correct AKM for the client that has undergone SAE authentication, use the following command.

```
Device# show wireless client mac-address <e0ca.94c9.6be0> detail

Client MAC Address : e0ca.94c9.6be0
!
!
!
Wireless LAN Name: WPA3

!
!
!
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
!
!
!
```

To view the correct AKM for the client that has undergone OWE authentication, use the following command.

```
Device# show wireless client mac-address <e0ca.94c9.6be0> detail

Client MAC Address : e0ca.94c9.6be0
!
!
!
Wireless LAN Name: WPA3

!
!
!
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : OWE
!
!
!
```

To view the list of PMK cache stored locally, use the following command.

```
Device# show wireless pmk-cache

Number of PMK caches in total : 0

Type      Station             Entry Lifetime  VLAN Override         IP Override
Audit-Session-Id              Username
------------------------------------------------------------------------------
```

Verifying WPA3 SAE H2E Support in WLAN

To view the WLAN properties (PWE method) based on the WLAN ID, use the following command:

```
Device# show wlan id 1
WLAN Profile Name     : wpa3
================================================
Identifier                                       : 1
Description                                      :
Network Name (SSID)                              : wpa3
Status                                           : Enabled
Broadcast SSID                                   : Enabled
Advertise-Apname                                 : Disabled
Universal AP Admin                               : Disabled
Max Associated Clients per WLAN                  : 0
Max Associated Clients per AP per WLAN           : 0
Max Associated Clients per AP Radio per WLAN     : 200
OKC                                              : Enabled
Number of Active Clients                         : 0
CHD per WLAN                                     : Enabled
WMM                                              : Allowed
WiFi Direct Policy                               : Disabled
Channel Scan Defer Priority:
  Priority (default)                             : 5
  Priority (default)                             : 6
Scan Defer Time (msecs)                          : 100
Media Stream Multicast-direct                    : Disabled
CCX - AironetIe Support                          : Disabled
Peer-to-Peer Blocking Action                     : Disabled
DTIM period for 802.11a radio                    : 1
DTIM period for 802.11b radio                    : 1
Local EAP Authentication                         : Disabled
Mac Filter Authorization list name               : Disabled
Mac Filter Override Authorization list name      : Disabled
Accounting list name                             :
802.1x authentication list name                  : Disabled
802.1x authorization list name                   : Disabled
Security
    802.11 Authentication                        : Open System
    Static WEP Keys                              : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)       : Enabled
        WPA (SSN IE)                             : Disabled
        WPA2 (RSN IE)                            : Disabled
        WPA3 (WPA3 IE)                           : Enabled
            AES Cipher                           : Enabled
            CCMP256 Cipher                       : Disabled
            GCMP128 Cipher                       : Disabled
            GCMP256 Cipher                       : Disabled
        Auth Key Management
            802.1x                               : Disabled
            PSK                                  : Disabled
            CCKM                                 : Disabled
            FT dot1x                             : Disabled
            FT PSK                               : Disabled
            Dot1x-SHA256                         : Disabled
            PSK-SHA256                           : Disabled
            SAE                                  : Enabled
            OWE                                  : Disabled
            SUITEB-1X                            : Disabled
            SUITEB192-1X                         : Disabled
    SAE PWE Method                               : Hash to Element(H2E)
    Transition Disable                           : Disabled
```

```
    CCKM TSF Tolerance (msecs)                 : 1000
    OWE Transition Mode                        : Disabled
    OSEN                                       : Disabled
    FT Support                                 : Disabled
        FT Reassociation Timeout (secs)        : 20
        FT Over-The-DS mode                    : Disabled
    PMF Support                                : Required
        PMF Association Comeback Timeout (secs): 1
        PMF SA Query Time (msecs)              : 200
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : Disabled
    Webauth Authorization List Name            : Disabled
    Webauth Parameter Map                      : Disabled
Band Select                                    : Disabled
Load Balancing                                 : Disabled
Multicast Buffer                               : Disabled
Multicast Buffers (frames)                     : 0
IP Source Guard                                : Disabled
Assisted-Roaming
    Neighbor List                              : Enabled
    Prediction List                            : Disabled
    Dual Band Support                          : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                 : Enabled
    BSS Max Idle                               : Enabled
        Protected Mode                         : Disabled
    Traffic Filtering Service                  : Disabled
    BSS Transition                             : Enabled
        Disassociation Imminent                : Disabled
            Optimised Roaming Timer (TBTTS)    : 40
            Timer (TBTTS)                      : 200
        Dual Neighbor List                     : Disabled
    WNM Sleep Mode                             : Disabled
802.11ac MU-MIMO                               : Enabled
802.11ax parameters
    802.11ax Operation Status                  : Enabled
    OFDMA Downlink                             : Enabled
    OFDMA Uplink                               : Enabled
    MU-MIMO Downlink                           : Enabled
    MU-MIMO Uplink                             : Enabled
    BSS Target Wake Up Time                    : Enabled
    BSS Target Wake Up Time Broadcast Support  : Enabled
802.11 protocols in 2.4ghz band
    Protocol                                   : dot11bg
Advanced Scheduling Requests Handling          : Enabled
mDNS Gateway Status                            : Bridge
WIFI Alliance Agile Multiband                  : Disabled
Device Analytics
    Advertise Support                          : Enabled
    Advertise Support for PC analytics         : Enabled
    Share Data with Client                     : Disabled
Client Scan Report (11k Beacon Radio Measurement)
    Request on Association                     : Disabled
    Request on Roam                            : Disabled
WiFi to Cellular Steering                      : Disabled
Advanced Scheduling Requests Handling          : Enabled
Locally Administered Address Configuration
    Deny LAA clients                           : Disabled
```

To verify the client association who have used the PWE method as H2E or HnP, use the following command:

```
Device# show wireless client mac-address e884.a52c.47a5 detail
Client MAC Address : e884.a52c.47a5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 11.11.0.65
Client IPv6 Addresses : fe80::c80f:bb8c:86f6:f71f
Client Username: N/A
AP MAC Address : d4ad.bda2.e9e0
AP Name: APA453.0E7B.E73C
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : N/A
Wireless LAN Id: 1
WLAN Profile Name: wpa3
Wireless LAN Network Name (SSID): wpa3
BSSID : d4ad.bda2.e9ef
Connected For : 72 seconds
Protocol : 802.11ax - 5 GHz
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 2
Authentication Algorithm : Simultaneous Authentication of Equals (SAE)
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1728 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m6 ss2
Supported Rates : 6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 0 (kbps)
  QoS Realtime Average Data Rate Upstream    : 0 (kbps)
  QoS Burst Data Rate Upstream               : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
  QoS Average Data Rate Downstream           : 0 (kbps)
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 08/24/2021 04:39:47 Pacific
Client Join Time:
  Join Time Of Client : 08/24/2021 04:39:47 Pacific
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 72 seconds
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
AAA override passphrase : No
```

```
SAE PWE Method : Hash to Element(H2E)
Transition Disable Bitmap : None
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : Yes
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : VLAN0011
Multicast VLAN : 0
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90000006
  IIF ID              : 0x90000006
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 000000000000000C76750C17
  Acct Session ID  : 0x00000000
  Auth Method Status List
   Method : SAE
  Local Policies:
   Service Template : wlan_svc_default-policy-profile_local (priority 254)
    VLAN              : VLAN0011
    Absolute-Timer    : 1800
  Server Policies:
  Resultant Policies:
                VLAN Name        : VLAN0011
    VLAN              : 11
    Absolute-Timer    : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Implemented
11v DMS Capable : No
QoS Map Capable : Yes
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
Client Statistics:
  Number of Bytes Received from Client : 21757
  Number of Bytes Sent to Client : 4963
  Number of Packets Received from Client : 196
  Number of Packets Sent to Client : 37
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -72 dBm
  Signal to Noise Ratio : 20 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: Neighbor Report, Passive Beacon Measurement, Active Beacon Measurement,
Table Beacon Measurement
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
```

To view the number of SAE authentications using the H2E and HnP, use the following command:

```
Device# show wireless stats client detail
Total Number of Clients : 0

Protocol Statistics

--------------------------------------------------------------------------------
Protcol            Client Count
 802.11b              : 0
 802.11g              : 0
 802.11a              : 0
 802.11n-2.4GHz       : 0
 802.11n-5 GHz        : 0
 802.11ac             : 0
 802.11ax-5 GHz       : 0
 802.11ax-2.4 GHz     : 0
  802.11ax-6 GHz      : 0



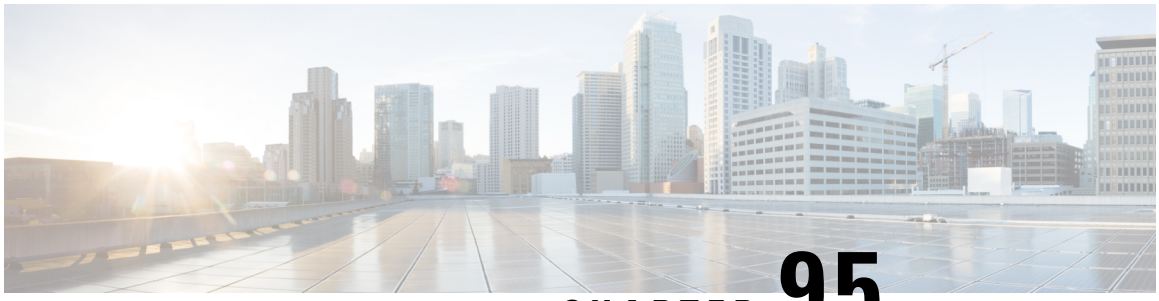
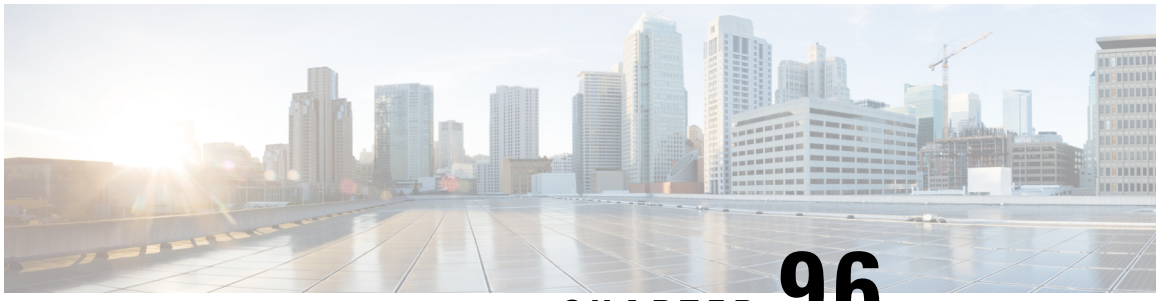
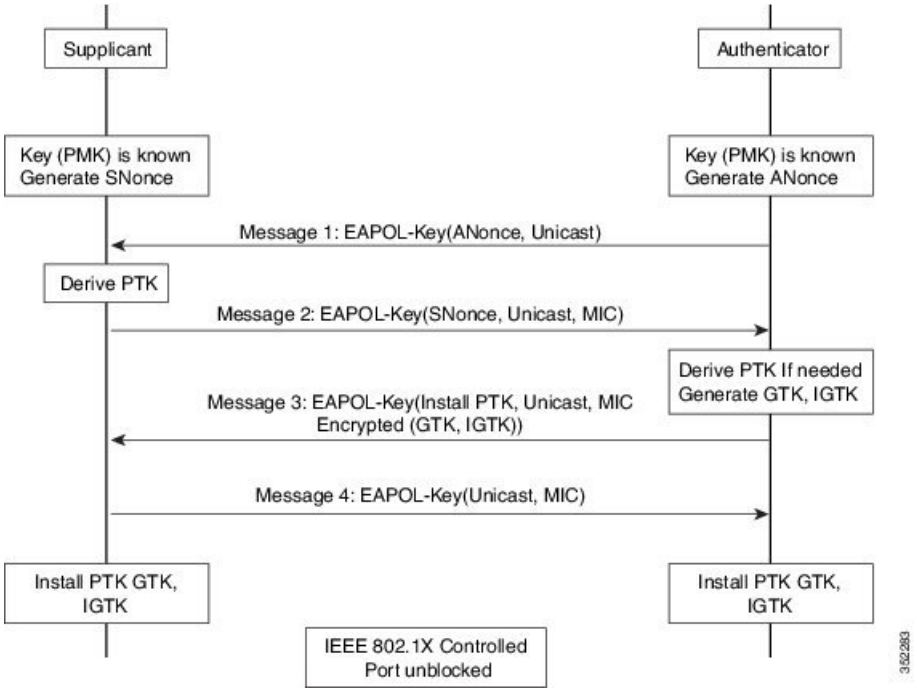
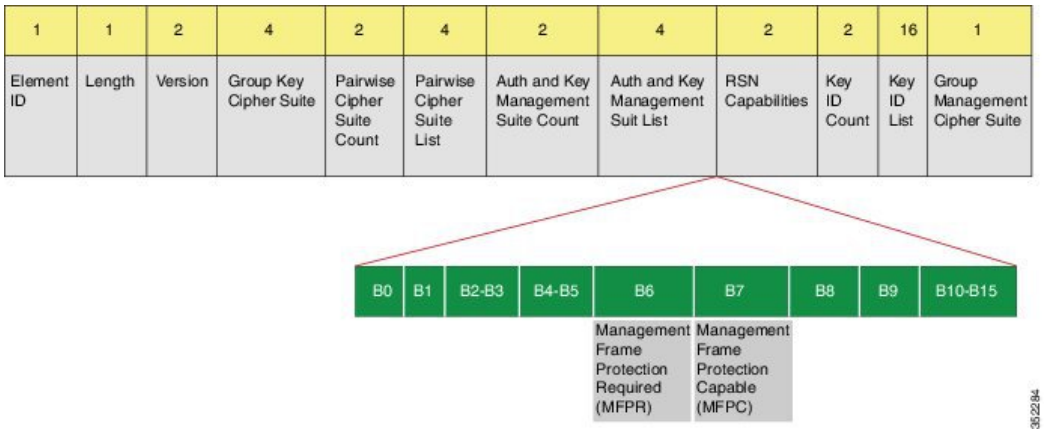
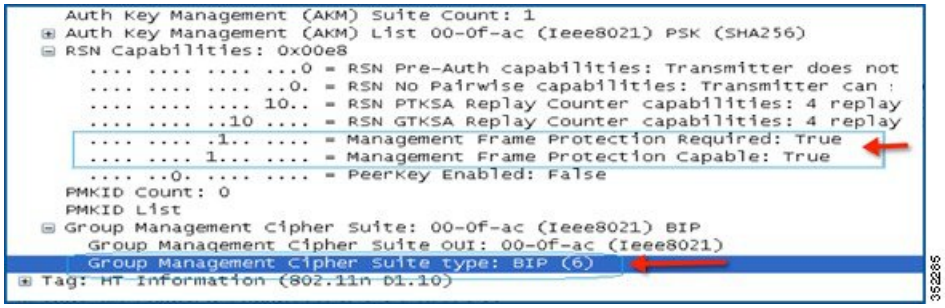
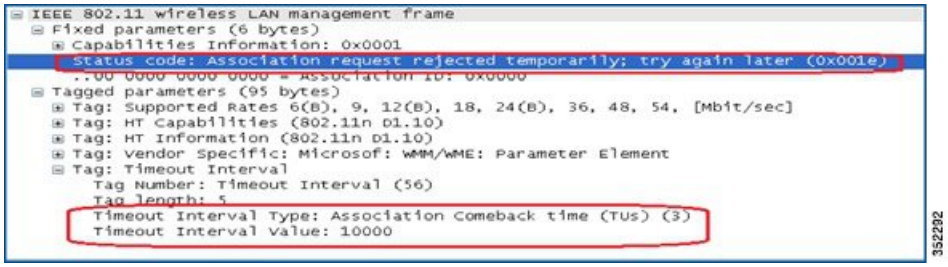
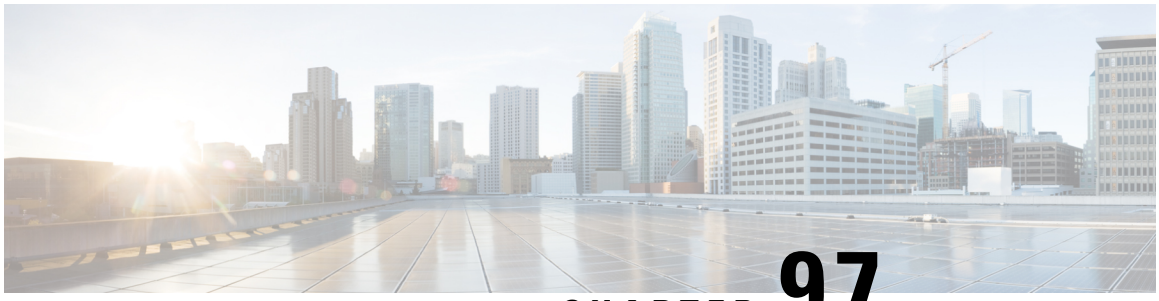
Current client state statistics:
--------------------------------------------------------------------------------
  Authenticating         : 0
  Mobility               : 0
  IP Learn               : 0
  Webauth Pending        : 0
  Run                    : 0
  Delete-in-Progress     : 0


Client Summary
-----------------------------
Current Clients : 0
Excluded Clients: 0
Disabled Clients: 0
Foreign Clients : 0
Anchor Clients  : 0
Local Clients   : 0
Idle Clients    : 0
Locally Administered MAC Clients: 0

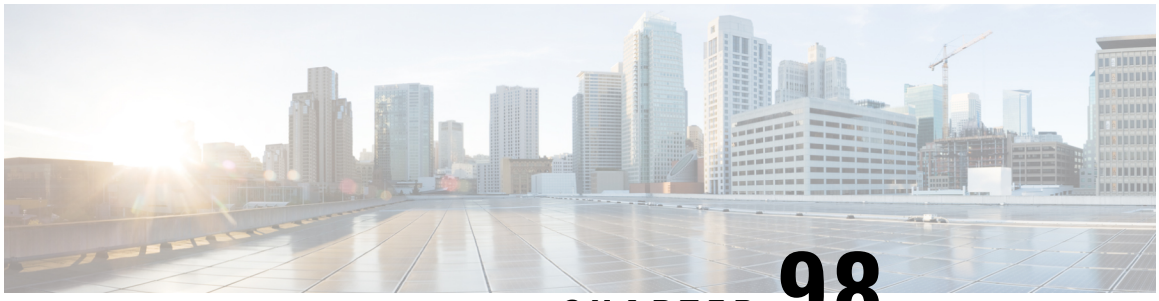
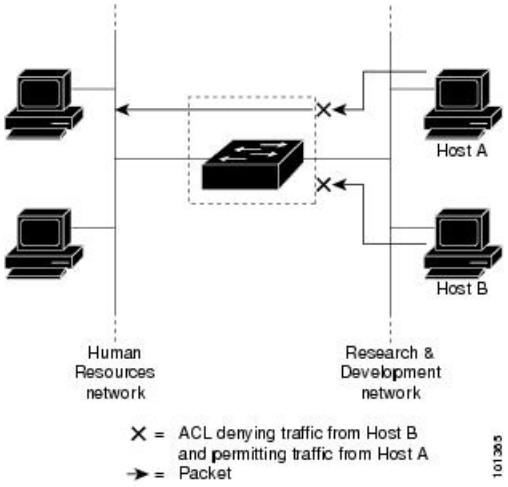
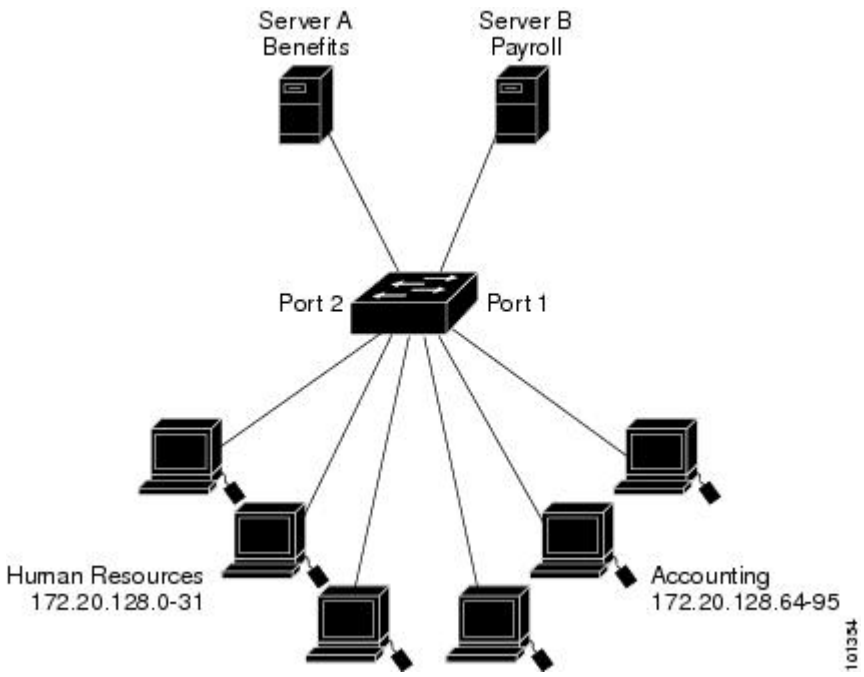
client global statistics:
--------------------------------------------------------------------------------
Total association requests received              : 0
Total association attempts                       : 0
Total FT/LocalAuth requests                      : 0
Total association failures                       : 0
Total association response accepts               : 0
Total association response rejects               : 0
Total association response errors                : 0
Total association failures due to exclusion list      : 0
Total association drops due to multicast mac     : 0
Total association drops due to random mac        : 0
Total association drops due to throttling        : 0
Total association drops due to unknown bssid     : 0
Total association drops due to parse failure     : 0
Total association drops due to other reasons     : 0
Total association requests wired clients         : 0
Total association drops wired clients            : 0
Total association success wired clients          : 0
Total peer association requests wired clients    : 0
Total peer association drops wired clients       : 0
Total peer association success wired clients     : 0
```

```
Total association success wifi direct clients    : 0
Total association rejects wifi direct clients    : 0
Total association response errors                 : 0
Total 11r ft authentication requests received    : 0
Total 11r ft authentication response success     : 0
Total 11r ft authentication response failure     : 0
Total 11r ft action requests received            : 0
Total 11r ft action response success             : 0
Total 11r ft action response failure             : 0
Total 11r PMKR0-Name mismatch                    : 0
Total 11r PMKR1-Name mismatch                    : 0
Total 11r MDID mismatch                          : 0
Total AID allocation failures                    : 0
Total AID free failures                          : 0
Total Roam Across Policy Profiles                : 0
Total roam attempts                              : 0
  Total CCKM roam attempts                       : 0
  Total 11r roam attempts                        : 0
  Total 11r slow roam attempts                   : 0
  Total 11i fast roam attempts                   : 0
  Total 11i slow roam attempts                   : 0
  Total other roam type attempts                 : 0
Total roam failures in dot11                     : 0

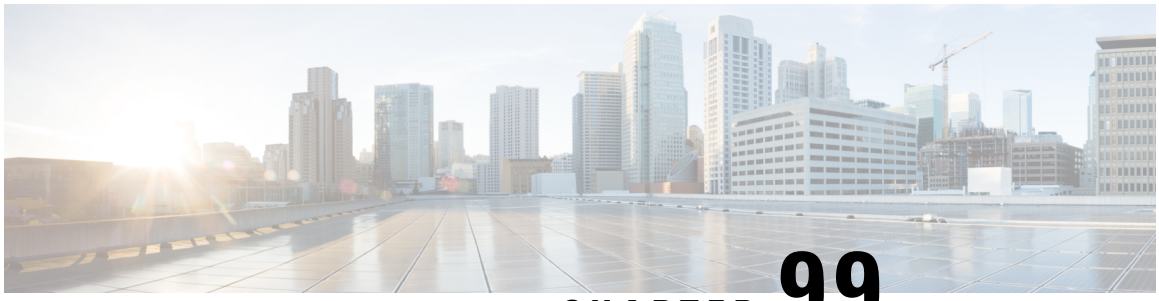
Total WPA3 SAE attempts                          : 0
Total WPA3 SAE successful authentications        : 0
Total WPA3 SAE authentication failures           : 0
  Total incomplete protocol failures             : 0
Total WPA3 SAE commit messages received          : 0
Total WPA3 SAE commit messages rejected                                    : 0
  Total unsupported group rejections                                       : 0
  Total PWE method mismatch for SAE Hash to Element commit received        : 0
  Total PWE method mismatch for SAE Hunting And Pecking commit received : 0
Total WPA3 SAE commit messages sent              : 0
Total WPA3 SAE confirm messages received         : 0
Total WPA3 SAE confirm messages rejected         : 0
  Total WPA3 SAE message confirm field mismatch  : 0
  Total WPA3 SAE confirm message invalid length  : 0
Total WPA3 SAE confirm messages sent             : 0
Total WPA3 SAE Open Sessions                     : 0
Total SAE Message drops due to throttling        : 0
Total WPA3 SAE Hash to Element commit received   : 0
Total WPA3 SAE Hunting and Pecking commit received : 0

Total Flexconnect local-auth roam attempts       : 0
  Total AP 11i fast roam attempts                : 0
  Total AP 11i slow roam attempts                : 0
  Total 11r flex roam attempts                   : 0
```

Verifying WPA3 Transition Disable in WLAN

To view the WLAN properties (transition disable) based on the WLAN ID, use the following command:

```
Device# show wlan id 7

WLAN Profile Name     : wl-sae
================================================
Identifier                                       : 7
Description                                      :
Network Name (SSID)                              : wl-sae
Status                                           : Enabled
Broadcast SSID                                   : Enabled
```

```
Advertise-Apname                                : Disabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
OKC                                             : Enabled
Number of Active Clients                        : 0
CHD per WLAN                                    : Enabled
WMM                                             : Allowed
WiFi Direct Policy                              : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Disabled
Peer-to-Peer Blocking Action                    : Disabled
Configured Radio Bands                          : All
Operational State of Radio Bands
    2.4ghz                                      : UP
    5ghz                                        : UP
DTIM period for 802.11a radio                   :
DTIM period for 802.11b radio                   :
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Mac Filter Override Authorization list name     : Disabled
Accounting list name                            :
802.1x authentication list name                 : Disabled
802.1x authorization list name                  : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            MPSK                                : Disabled
            EasyPSK                             : Disabled
            AES Cipher                          : Enabled
            CCMP256 Cipher                      : Disabled
            GCMP128 Cipher                      : Disabled
            GCMP256 Cipher                      : Disabled
            Randomized GTK                      : Disabled
        WPA3 (WPA3 IE)                          : Enabled
            AES Cipher                          : Enabled
            CCMP256 Cipher                      : Disabled
            GCMP128 Cipher                      : Disabled
            GCMP256 Cipher                      : Disabled
        Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Enabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            Dot1x-SHA256                        : Disabled
            PSK-SHA256                          : Disabled
            SAE                                 : Enabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    Transition Disable                          : Enabled
    CCKM TSF Tolerance (msecs)                  : 1000
```

To verify the client association who have used the transition disable, use the following command:

```
Device# show wireless client mac-address 2c33.7a5b.8fc5 detail
Client MAC Address : 2c33.7a5b.8fc5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 166.166.1.101
Client Username: N/A
AP MAC Address : 7c21.0d48.ed00
AP Name: APF4BD.9EBD.A66C
AP slot : 0
Client State : Associated
Policy Profile : po-sae
Flex Profile : N/A
Wireless LAN Id: 7
WLAN Profile Name: wl-sae
Wireless LAN Network Name (SSID): wl-sae
BSSID : 7c21.0d48.ed02
Connected For : 15 seconds
Protocol : 802.11n - 2.4 GHz
Channel : 11
Client IIF-ID : 0xa0000002
Association Id : 1
Authentication Algorithm : Simultaneous Authentication of Equals (SAE)
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1787 sec)
Session Warning Time : Timer not running
Input Policy Name : None
Input Policy State : None
Input Policy Source : None
Output Policy Name : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : In-Active
Power Save : OFF
Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
QoS Average Data Rate Upstream : 0 (kbps)
QoS Realtime Average Data Rate Upstream : 0 (kbps)
QoS Burst Data Rate Upstream : 0 (kbps)
QoS Realtime Burst Data Rate Upstream : 0 (kbps)
QoS Average Data Rate Downstream : 0 (kbps)
QoS Realtime Average Data Rate Downstream : 0 (kbps)
QoS Burst Data Rate Downstream : 0 (kbps)
QoS Realtime Burst Data Rate Downstream : 0 (kbps)
Mobility:
Move Count : 0
Mobility Role : Local
Mobility Roam Type : None
Mobility Complete Timestamp : 05/16/2021 11:18:14 UTC
Client Join Time:
Join Time Of Client : 05/16/2021 11:18:14 UTC
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 15 seconds
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
AAA override passphrase : No
Transition Disable Bitmap : 0x01
User Defined (Private) Network : Disabled
```

```
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : Yes
```



CHAPTER 95

IP Source Guard

- Information About IP Source Guard, on page 1081
- Configuring IP Source Guard (GUI), on page 1081
- Configuring IP Source Guard, on page 1082

Information About IP Source Guard

IP Source Guard (IPSG) is a Layer 2 security feature in the Cisco Catalyst 9800 Series Wireless Controller . It supports both IPv4 and IPv6 wireless clients.

The IPSG feature prevents the wireless controller from forwarding the packets, with the source IP addresses that are not known to it. This security feature is not enabled by default and has to be explicitly configured. It is enabled on a per WLAN basis, and all the wireless clients joining that WLAN inherits this feature.

The wireless controller maintains an IP/MAC pair binding table for the IPSG feature. Using this table, the wireless controller keeps track of IP and MAC address combination (binding) information for all the wireless clients. This binding information is captured as part of the IP learning process. When the feature is enabled on a WLAN, the wireless controller forwards the incoming packets (from the wireless clients) only if it finds a matching binding table entry corresponding to the source IP and MAC address combination of those packets. Otherwise, the packets are dropped.

Configuring IP Source Guard (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click the WLAN.

Step 3 In the **Advanced** tab, check the **IP Source Guard** checkbox.

Step 4 Click **Update & Apply to Device**.

Configuring IP Source Guard

Follow the procedure given below to configure IPSG:

Before you begin

Cisco Catalyst 9800 Series Wireless Controller supports only one IPv4 address for a client and up to 8 IPv6 addresses (including link local addresses) per client.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID to use. **Note** If a WLAN is not already configured, this step creates the WLAN.
Step 2	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 3	**ip verify source mac-check** **Example:** `Device(config-wlan)# ip verify source mac-check`	Enables the IP Source Guard feature.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.



CHAPTER 96

802.11w

- Information About 802.11w, on page 1083
- Prerequisites for 802.11w, on page 1086
- Restrictions for 802.11w, on page 1086
- How to Configure 802.11w, on page 1087
- Disabling 802.11w, on page 1088
- Monitoring 802.11w, on page 1089

Information About 802.11w

Wi-Fi is a broadcast medium that enables any device to eavesdrop and participate either as a legitimate or rogue device. Management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and tear down sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, an attacker could spoof management frames from an AP to attack a client associated with the AP.

The 802.11w protocol applies only to a set of robust management frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, De-authentication, and Robust Action frames.

Management frames that are considered as robust action and therefore protected are the following:

- Spectrum Management
- QoS
- DLS
- Block Ack
- Radio Measurement
- Fast BSS Transition
- SA Query
- Protected Dual of Public Action
- Vendor-specific Protected

When 802.11w is implemented in the wireless medium, the following occur:

- Client protection is added by the AP adding cryptographic protection to de-authentication and dissociation frames preventing them from being spoofed in a DOS attack.
- Infrastructure protection is added by adding a Security Association (SA) tear down protection mechanism consisting of an Association Comeback Time and an SA-Query procedure preventing spoofed association request from disconnecting an already connected client.

802.11w has introduced a new IGTK Key, which is used to protect broadcast/multicast robust management frames:

- IGTK is a random value assigned by the authenticator STA (WLC) and used to protect MAC management protocol data units (MMPDUs) from that source STA.

When Management Frame Protection is negotiated, the AP encrypts the GTK and IGTK values in the EAPOL-Key frame, which is delivered in Message 3 of 4-way handshake.

Figure 33: IGTK Exchange in 4-way Handshake



- If the AP later changes the GTK, it sends the new GTK and IGTK to the client using the Group Key Handshake .

802.11w defines a new Broadcast/Multicast Integrity Protocol (BIP) that provides data integrity and replay protection for broadcast/multicast robust management frames after successful establishment of an IGTKSA - It adds a MIC that is calculated using the shared IGTK key.

802.11w Information Elements (IEs)

Figure 34: 802.11w Information Elements



1. Modifications made in the RSN capabilities field of RSNIE.
   a. Bit 6: Management Frame Protection Required (MFPR)
   b. Bit 7: Management Frame Protection Capable (MFPC)
2. Two new AKM Suites, 5 and 6 are added for AKM Suite Selectors.
3. New Cipher Suite with type 6 is added to accommodate BIP.

The WLC adds this modified RSNIE in association and re-association responses and the APs add this modified RSNIE in beacons and probe responses.

The following Wireshark captures shows the RSNIE capabilities and the Group Management Cipher Suite elements.

Figure 35: 802.11w Information Elements



Security Association (SA) Teardown Protection

SA teardown protection is a mechanism to prevent replay attacks from tearing down the session of an existing client. It consists of an Association Comeback Time and an SA-Query procedure preventing spoofed association requests from disconnecting an already connected client.

If a client has a valid security association, and has negotiated 802.11w, the AP shall reject another Association Request with status code 30. This status code stands for "Association request rejected temporarily; Try again later". The AP should not tear down or otherwise modify the state of the existing association until the SA-Query

procedure determines that the original SA is invalid and shall include in the Association Response an Association Comeback Time information element, specifying a comeback time when the AP would be ready to accept an association with this client.

The following capture shows the Association Reject message with status code 0x1e (30) and the Association comeback time set to 10 seconds.

Figure 36: Association Reject with Comeback Time



Following this, if the AP is not already engaged in an SA Query with the client, the AP shall issue an SA Query until a matching SA Query response is received or the Association Comeback time expires. An AP may interpret reception of a valid protected frame as an indication of a successfully completed SA Query.

If a SA QUERY response with a matching transaction identifier within the time period, the AP shall allow the association process to be started without starting additional SA Query procedures.

Prerequisites for 802.11w

- To configure 802.11w feature for optional and mandatory, you must have WPA and AKM configured.

Note The RNS (Robust Secure Network) IE must be enabled with an AES Cipher.

Restrictions for 802.11w

- 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN.
- Cisco Catalyst 9800 Series Wireless Controller supports 802.11w + PMF combination for non-Apple clients. But Apple iOS version 11 and earlier require fix from the Apple iOS side to resolve the association issues.
- The controller will ignore disassociation or deauthentication frames sent by the clients if they are not using 802.11w PMF. The client entry will only get deleted immediately upon reception of such a frame if the client uses PMF. This is to avoid denial of service by malicious device since there is no security on those frames without PMF.

How to Configure 802.11w

Configuring 802.11w (GUI)

Before you begin

WPA and AKM must be configured.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add** to create WLANs.

The **Add WLAN** page is displayed.

Step 3 In the **Security** > **Layer2** tab, navigate to the **Protected Management Frame** section.

Step 4 Choose **PMF** as *Disabled*, *Optional*, or *Required*. By default, the PMF is *disabled*.

If you choose **PMF** as *Optional* or *Required*, you get to view the following fields:

- **Association Comeback Timer**—Enter a value between 1 and 10 seconds to configure 802.11w association comeback time.
- **SA Query Time**—Enter a value between 100 to 500 (milliseconds). This is required for clients to negotiate 802.11w PMF protection on a WLAN.

Step 5 Click **Save & Apply to Device**.

Configuring 802.11w (CLI)

Before you begin

WPA and AKM must be configured.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan wlan-test 12 alpha`	Configures a WLAN and enters configuration mode.

	Command or Action	Purpose
Step 3	**security wpa akm dot1x-sha256** **Example:** `Device(config-wlan)#security wpa akm dot1x-sha256`	Configures 802.1x support.
Step 4	**security pmf association-comeback** *comeback-interval* **Example:** `Device(config-wlan)# security pmf association-comeback 10`	Configures the 802.11w association comeback time.
Step 5	**security pmf mandatory** **Example:** `Device(config-wlan)# security pmf mandatory`	Requires clients to negotiate 802.11w PMF protection on a WLAN.
Step 6	**security pmf saquery-retry-time** *timeout* **Example:** `Device(config-wlan)# security pmf saquery-retry-time 100`	Time interval identified in milliseconds before which the SA query response is expected. If the device does not get a response, another SQ query is tried.

Disabling 802.11w

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan wlan-test 12 alpha`	Configures a WLAN and enters configuration mode.
Step 3	**no security wpa akm dot1x-sha256** **Example:** `Device(config-wlan)# no security wpa akm dot1x-sha256`	Disables 802.1x support.
Step 4	**no security pmf association-comeback** *comeback-interval* **Example:** `Device(config-wlan)# no security pmf association-comeback 10`	Disables the 802.11w association comeback time.

	Command or Action	Purpose
Step 5	**no security pmf mandatory** **Example:** `Device(config-wlan)# no security pmf mandatory`	Disables client negotiation of 802.11w PMF protection on a WLAN.
Step 6	**no security pmf saquery-retry-time** *timeout* **Example:** `Device(config-wlan)# no security pmf saquery-retry-time 100`	Disables SQ query retry.

Monitoring 802.11w

Use the following commands to monitor 802.11w.

Procedure

Step 1 **show wlan name** *wlan-name*

Displays the WLAN parameters on the WLAN. The PMF parameters are displayed.

```
. . . .
. . . .
Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Disabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            FT SAE                              : Disabled
            Dot1x-SHA256                        : Enabled
            PSK-SHA256                          : Disabled
            SAE                                 : Disabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Adaptive
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Required
        PMF Association Comeback Timeout        : 1
        PMF SA Query Time                       : 500
. . . .
. . . .
```

Step 2 **show wireless client mac-address** *mac-address* **detail**

Displays the summary of the 802.11w authentication key management configuration on a client.

```
. . . .
. . . .
Policy Manager State: Run
```

```
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 497 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x-SHA256
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : Yes
EAP Type : LEAP
VLAN : 39
Multicast VLAN : 0
Access VLAN : 39
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
. . . .
. . . .
```



CHAPTER 97

Management Frame Protection

- Information About Management Frame Protection, on page 1091
- Restrictions for Management Frame Protection, on page 1092
- Configuring Management Frame Protection (CLI), on page 1093
- Verifying Management Frame Protection Settings, on page 1093

Information About Management Frame Protection

By default, 802.11 management frames are unauthenticated and hence not protected against spoofing. Infrastructure management frame protection (MFP) and 802.11w protected management frames (PMF) provide protection against such attacks.

Infrastructure MFP

Infrastructure MFP protects management frames by detecting adversaries that are invoking denial-of-service attacks, flooding the network with associations and probes, interjecting as rogue APs, and affecting network performance by attacking the QoS and radio measurement frames. Infrastructure MFP is a global setting that provides a quick and effective means to detect and report phishing incidents.

Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by APs (and not those emitted by clients), which are then validated by other APs in the network. Infrastructure MFP is passive, can detect and report intrusions but has no means to stop them.

Infrastructure MFP consists of three main components:

- **Management frame protection**: The AP protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving AP configured to detect MFP frames to report the discrepancy. MFP is supported for use with Cisco Aironet lightweight APs.
- **Management frame validation**: In infrastructure MFP, the AP validates every management frame that it receives from other APs in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an AP that is configured to transmit MFP frames, it reports the discrepancy to the network management system. In order for the timestamps to operate properly, all controllers must be Network Time Protocol (NTP) synchronized.

- **Event reporting**: The AP notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and can report the results through SNMP traps to the network management system.

Infrastructure MFP is disabled by default, and you can enable it globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if you have enabled AP authentication because the two features are mutually exclusive. When you enable infrastructure MFP globally, signature generation (adding MICs to outbound frames) can be disabled for selected WLANs, and validation can be disabled for selected APs.

Note CCXv5 client MFP is no longer supported. Client MFP is enabled as optional by default on WLANs that are configured for WPA2. However, client MFP is not supported on Wave 2 APs or 802.11ax Wi-Fi6 APs, and there exist no clients that support CCXv5.

Supported Access Point Models

Cisco MFP is supported on the following AP models:

- Cisco Aironet 2802, 3802, and 4802 series access points
- Cisco Aironet 2800, 3800, 4800, and 1560 series access points

Unsupported Access Point Models

Cisco MFP is not supported on the following AP models:

- Cisco Aironet 1800 series access points
- Cisco 802.11ax access points
- All Cisco IOS access points

Restrictions for Management Frame Protection

- Lightweight access points support infrastructure MFP in local and monitor modes and in FlexConnect mode when the access point is connected to a controller.
- Client MFP is supported for use only with CCXv5 clients using WPA2 with TKIP or AES-CCMP.
- Client MFP is not supported on Cisco Wave 1 APs and Cisco Wave 2 APs.
- 802.11ax access points do not support MFP.
- Non-CCXv5 clients may associate to a WLAN, if client MFP is disabled or optional.
- Error reports generated on a FlexConnect access point in standalone mode cannot be forwarded to the controller and are dropped.
- Keys are generated using random number generator but you can improve the keys by changing to SHA.
- MFP key for each BSSID is not supported.

Configuring Management Frame Protection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps mfp** **Example:** `Device(config)# wireless wps mfp`	Configures a management frame protection.

Step 3	**wireless wps mfp** {**ap-impersonation** | **key-refresh-interval**}
	Example:
	`Device(config)# wireless wps mfp ap-impersonation`
	`Device(config)# wireless wps mfp key-refresh-interval`
		Configures ap impersonation detection (or) MFP key refresh interval in hours.
		key-refresh-interval—Refers to the MFP key refresh interval in hours. The valid range is from 1 to 24. Default value is 24.

Step 4	**end** **Example:** `Device(config)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Verifying Management Frame Protection Settings

To verify if the Management Frame Protection (MFP) feature is enabled or not, use the following command:

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

To view the MFP details, use the following command:

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
```

```
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

To view the MFP statistics details, use the following command:

```
Device# show wireless wps mfp statistics
BSSID          Radio DetectorAP                        LastSourceAddr Error           Count
     FrameTypes

aabb.ccdd.eeff a     AP3800                            aabb.ccdd.eeff Invalid MIC     10
     Beacon, Probe Response
                                                                     Invalid MIC     20
     Beacon, Probe Response
```

To verify if access points support MFP validation and protection, use the following command:

```
Device# show wireless wps mfp ap summary
AP Name                          Radio MAC               Validation            Protection
-------------------------------------------------------------------------------------------
AP002A.1087.CBF4                 00a2.eefd.bdc0          Enabled               Enabled
AP58AC.78DE.9946                 00a2.eeb8.4ae0          Enabled               Enabled
APb4de.3196.caac                 4c77.6d83.6b90          Enabled               Enabled
```



CHAPTER 98

IPv4 ACLs

- Information about Network Security with ACLs, on page 1095
- Restrictions for Configuring IPv4 Access Control Lists, on page 1103
- How to Configure ACLs, on page 1104
- Configuration Examples for ACLs, on page 1117
- Monitoring IPv4 ACLs, on page 1121

Information about Network Security with ACLs

This chapter describes how to configure network security on the switch by using access control lists (ACLs), which in commands and tables are also referred to as access lists.

ACL Overview

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a controller and permit or deny packets crossing specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the controller accepts or rejects the packets. Because the controller stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the controller rejects the packet. If there are no restrictions, the controller forwards the packet; otherwise, the controller drops the packet. The controller can use ACLs on all packets it forwards. There is implcit any host deny deny rule.

You configure access lists on a controller to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic.

Access Control Entries

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions the packet must satisfy in order to match the ACE. The meaning of *permit* or *deny* depends on the context in which the ACL is used.

Note The maximum number of ACEs that can be applied under an access policy (ACL) for central switching is 256 ACEs. The maximum number of ACEs applicable for Flex Mode or Local Switching is 64 ACEs.

ACL Supported Types

The switch supports IP ACLs and Ethernet (MAC) ACLs:

- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- Ethernet ACLs filter non-IP traffic.

This switch also supports quality of service (QoS) classification ACLs.

Supported ACLs

The controller supports three types of ACLs to filter traffic:

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply port ACLs to a Layer 2 interface in each direction to each access list type — IPv4 and MAC.
- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound).
- FQDN ACL: FQDN ACL is encoded along with IPv6 ACL and sent to AP. FQDN ACL is always a custom ACL. AP does DNS snooping and sends the IPv4 and IPv6 addresses to the controller.

ACL Precedence

When Port ACLs, and router ACLs are configured on the same switch, the filtering precedence, from greatest to least for ingress traffic is port ACL, and then router ACL. For egress traffic, the filtering precedence is router ACL, and then port ACL.

The following examples describe simple use cases:

- When an input router ACL and input port ACL exist in a switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.

Port ACLs

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

The switch examines ACLs on an interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs control access to a network or to part of a network.

Figure 37: Using ACLs to Control Traffic in a Network



This is an example of using port ACLs to control access to a network when all workstations are in the same VLAN. ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network. Port ACLs can only be applied to Layer 2 interfaces in the inbound direction.

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.

Note You can't apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

Router ACLs

You can apply router ACLs on switch virtual interfaces (SVIs), which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces. You apply router ACLs on interfaces for specific directions (inbound or outbound). You can apply one router ACL in each direction on an interface.

The switch supports these access lists for IPv4 traffic:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

As with port ACLs, the switch examines ACLs associated with features configured on a given interface. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL, and can be used to control access to a network or to part of a network.

ACEs and Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some access control entries (ACEs) do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.

Note For TCP ACEs with L4 Ops, the fragmented packets will be dropped per RFC 1858.

- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

ACEs and Fragmented and Unfragmented Traffic Examples

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
Device(config)# access-list 102 deny tcp any any
```

Note In the first and second ACEs in the examples, the *eq* keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

- Packet A is a TCP packet from host 10.2.2.2., port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.

- Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit).

  Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

- Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

Standard and Extended IPv4 ACLs

This section describes IP ACLs.

An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IPv4:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.

Note Only extended ACLs are supported while the standard ACLs are not supported.

IPv4 ACL Switch Unsupported Features

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers.

The following ACL-related features are not supported:

- Non-IP protocol ACLs
- IP accounting
- Reflexive ACLs, URL Redirect ACLs and Dynamic ACLs are not supported.

Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating.

This lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, numbers 1 to 199 and 1300 to 2699.

Table 75: Access List Numbers

Access List Number	Type	Supported
1–99	IP standard access list	Yes
100–199	IP extended access list	Yes
200–299	Protocol type-code access list	No
300–399	DECnet access list	No
400–499	XNS standard access list	No
500–599	XNS extended access list	No
600–699	AppleTalk access list	No
700–799	48-bit MAC address access list	No
800–899	IPX standard access list	No
900–999	IPX extended access list	No
1000–1099	IPX SAP access list	No
1100–1199	Extended 48-bit MAC address access list	No
1200–1299	IPX summary address access list	No
1300–1999	IP standard access list (expanded range)	Yes
2000–2699	IP extended access list (expanded range)	Yes

In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs by using the supported numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Numbered Standard IPv4 ACLs

When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

The switch always rewrites the order of standard access lists so that entries with **host** matches and entries with matches having a *don't care* mask of 0.0.0.0 are moved to the top of the list, above any entries with non-zero *don't care* masks. Therefore, in **show** command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to terminal lines (virtual teletype (VTY) lines), or to interfaces.

Numbered Extended IPv4 ACLs

Although standard ACLs use only source addresses for matching, you can use extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. When you are creating ACEs in numbered extended access lists, remember that after you create the ACL, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

The switch does not support dynamic or reflexive access lists. It also does not support filtering based on the type of service (ToS) minimize-monetary-cost bit.

Some protocols also have specific parameters and keywords that apply to that protocol.

You can define an extended TCP, UDP, ICMP, IGMP, or other IP ACL. The switch also supports these IP protocols:

These IP protocols are supported:

- Authentication Header Protocol (**ahp**)
- Encapsulation Security Payload (**esp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- generic routing encapsulation (**gre**)
- Internet Control Message Protocol (**icmp**)
- Internet Group Management Protocol (**igmp**)
- any Interior Protocol (**ip**)
- IP in IP tunneling (**ipinip**)
- KA9Q NOS-compatible IP over IP tunneling (**nos**)
- Open Shortest Path First routing (**ospf**)
- Payload Compression Protocol (**pcp**)
- Protocol-Independent Multicast (**pim**)
- Transmission Control Protocol (**tcp**)
- User Datagram Protocol (**udp**)

Named IPv4 ACLs

You can identify IPv4 ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IPv4 access lists in a router than if you were to use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, at times, not all commands that use IP access lists accept a named access list.

Note The name you give to a standard or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99 and . The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines before configuring named ACLs:

- Numbered ACLs are also available.
- A standard ACL and an extended ACL cannot have the same name.

ACL Logging

The controller software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the ACL causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** commands controlling the syslog messages.

Note Because routing is done in hardware and logging is done in software, if a large number of packets match a *permit* or *deny* ACE containing a **log** keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

The first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they appear or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

Note The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

Hardware and Software Treatment of IP ACLs

ACL processing is performed in hardware. If the hardware reaches its capacity to store ACL configurations, all packets on that interface are dropped.

The ACL scale for controllers is as follows:

- Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-CL Wireless Controller (small and medium) support 128 ACLs with 128 Access List Entries (ACEs).
- Cisco Catalyst 9800-80 Wireless Controller and Cisco Catalyst 9800-CL Wireless Controller (large) support 256 ACLs and 256 ACEs.
- FlexConnect and Fabric mode APs support 96 ACLs.

Note If an ACL configuration cannot be implemented in the hardware due to an out-of-resource condition on the controller, then only the traffic in that VLAN arriving on that controller is affected.

When you enter the **show ip access-lists** privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. Use the privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

IPv4 ACL Interface Considerations

For inbound ACLs, after receiving a packet, the controller checks the packet against the ACL. If the ACL permits the packet, the controller continues to process the packet. If the ACL rejects the packet, the controller discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the controller checks the packet against the ACL. If the ACL permits the packet, the controller sends the packet. If the ACL rejects the packet, the controller discards the packet.

If an undefined ACL has nothing listed in it, it is an empty access list.

Restrictions for Configuring IPv4 Access Control Lists

The following are restrictions for configuring network security with ACLs:

General Network Security

The following are restrictions for configuring network security with ACLs:

- A standard ACL and an extended ACL cannot have the same name.
- Though visible in the command-line help strings, **AppleTalk** is not supported as a matching condition for the **deny** and **permit** MAC access-list configuration mode commands.
- DNS traffic is permitted by default with or without ACL entries for clients that are awaiting web authentication.

IPv4 ACL Network Interfaces

The following restrictions apply to IPv4 ACLs to network interfaces:

- When controlling access to an interface, you can use a named or numbered ACL.
- You do not have to enable routing to apply ACLs to Layer 2 interfaces.

MAC ACLs on a Layer 2 Interface

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

- You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IP packets, and the MAC access list filters non-IP packets.
- A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.

Note The **mac access-group** interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

IP Access List Entry Sequence Numbering

- This feature does not support dynamic, reflexive, or firewall access lists.

How to Configure ACLs

Configuring IPv4 ACLs (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** dialog box, enter the following parameters.

- **ACL Name:** Enter the name for the ACL.
- **ACL Type:** IPv4 Standard.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Log:** Enable or disable logging.

Step 4 Click **Add**.

Step 5 Add the rest of the rules and click **Apply to Device**.

Configuring IPv4 ACLs

Follow the procedure given below to use IP ACLs on the switch:

Procedure

Step 1 Create an ACL by specifying an access list number or name and the access conditions.

Step 2 Apply the ACL to interfaces or terminal lines..

Creating a Numbered Standard ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 On the **ACL** page, click **Add**.

Step 3 In the **Add ACL Setup** window, enter the following parameters.

- **ACL Name:** Enter the name for the ACL.
- **ACL Type:** IPv4 Standard.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** access from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network**
- **Log:** Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.

Step 4 Click **Add**.

Step 5 Click **Save & Apply to Device**.

Creating a Numbered Standard ACL (CLI)

Follow the procedure given below to create a numbered standard ACL:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard*] **Example:** `Device(config)# access-list 2 deny`	Defines a standard IPv4 access list by using a source address and wildcard. The *access-list-number* is a decimal number from 1 to 99 or 1300 to 1999.

	Command or Action	Purpose
	`your_host`	Enter **deny** or **permit** to specify whether to deny or permit access if conditions are matched. The *source* is the source address of the network or host from which the packet is being sent specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** as an abbreviation for *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard. • The keyword **host** as an abbreviation for source and *source-wildcard* of *source* 0.0.0.0. (Optional) The *source-wildcard* applies wildcard bits to the source. **Note** Logging is supported only on ACLs attached to Layer 3 interfaces.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Creating a Numbered Extended ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 On the **ACL** page, click **Add**.

Step 3 In the **Add ACL Setup** window, enter the following parameters.

- **ACL Name:** Enter the name for the ACL.
- **ACL Type:** IPv4 Extended.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
- **Protocol:** Choose a protocol from the drop-down list.
- **Log:** Enable or disable logging.
- **DSCP:** Enter to match packets with the DSCP value

Step 4 Click **Add**.

Step 5 Click **Save & Apply to Device**.

Creating a Numbered Extended ACL (CLI)

Follow the procedure given below to create a numbered extended ACL:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** tos] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*]	Defines an extended IPv4 access list and the access conditions. The *access-list-number* is a decimal number from 100 to 199 or 2000 to 2699.

	Command or Action	Purpose
	Example: `Device(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log`	Enter **deny** or **permit** to specify whether to deny or permit the packet if conditions are matched. For *protocol*, enter the name or number of an P protocol: **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pcp**, **pim**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword **ip**. **Note** This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps. The *source* is the number of the network or host from which the packet is sent. The *source-wildcard* applies wildcard bits to the source. The *destination* is the network or host number to which the packet is sent. The *destination-wildcard* applies wildcard bits to the destination. Source, source-wildcard, destination, and destination-wildcard can be specified as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** for 0.0.0.0 255.255.255.255 (any host). • The keyword **host** for a single host 0.0.0.0. The other keywords are optional and have these meanings: • **precedence**—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), **network** (7). • **fragments**—Enter to check non-initial fragments. • **tos**—Enter to match by type of service level, specified by a number from 0 to 15

	Command or Action	Purpose
		or a name: **normal** (0), **max-reliability** (2), **max-throughput** (4), **min-delay** (8). • **time-range**—Specify the time-range name. • **dscp**—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values. **Note** Your controller must support the ability to: • Mark DCSP • Mark UP • Map DSCP and UP For more information on **DSCP-to-UP Mapping**, see: https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-01 **Note** If you enter a **dscp** value, you cannot enter **tos** or **precedence**. You can enter both a **tos** and a **precedence** value with no **dscp**.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*] **Example:** `Device(config)# access-list 101 permit tcp any any eq 500`	Defines an extended TCP access list and the access conditions. The parameters are the same as those described for an extended IPv4 ACL, with these exceptions: (Optional) Enter an *operator* and *port* to compare source (if positioned after *source source-wildcard*) or destination (if positioned after *destination destination-wildcard*) port. Possible operators include **eq** (equal), **gt** (greater than), **lt** (less than), **neq** (not equal), and **range** (inclusive range). Operators require a port number (range requires two port numbers separated by a space). Enter the *port* number as a decimal number (from 0 to 65535) or the name of a TCP port. Use only TCP port numbers or names when filtering TCP.

	Command or Action	Purpose
		The other optional keywords have these meanings: • *flag*—Enter one of these flags to match by the specified TCP header bits: **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
Step 4	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Device(config)# access-list 101 permit udp any any eq 100`	(Optional) Defines an extended UDP access list and the access conditions. The UDP parameters are the same as those described for TCP except that the [operator [port]] port number or name must be a UDP port number or name, and the **flag** not valid for UDP.
Step 5	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Device(config)# access-list 101 permit icmp any any 200`	Defines an extended ICMP access list and the access conditions. The ICMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings: • *icmp-type*—Enter to filter by ICMP message type, a number from 0 to 255. • *icmp-code*—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • *icmp-message*—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name.
Step 6	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] **Example:** `Device(config)# access-list 101 permit igmp any any 14`	(Optional) Defines an extended IGMP access list and the access conditions. The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter. *igmp-type*—To match IGMP message type, enter a number from 0 to 15, or enter the message name: **dvmrp**, **host-query**, **host-report**, **pim**, or **trace**.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Creating Named Standard ACLs (GUI)

Procedure

Step 1 Click **Configuration** > **Security** > **ACL**.

Step 2 Click **Add** to create a new ACL setup.

Step 3 In the **Add ACL Setup** window, enter the following parameters.

- **ACL Name:** Enter the name for the ACL
- **ACL Type:** IPv4 Standard
- **Sequence:** The valid range is between 1 and 99 or 1300 and 1999
- **Action:** Choose **Permit** or **Deny** access from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network**
- **Log:** Enable or disable logging, this is limited to ACLs associated to Layer 3 interface only.

Step 4 Click **Add** to add the rule.

Step 5 Click **Save & Apply to Device**.

Creating Named Standard ACLs

Follow the procedure given below to create a standard ACL using names:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**ip access-list standard** *name* **Example:** `Device(config)# ip access-list standard 20`	Defines a standard IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 1 to 99.

Step 4	Use one of the following:
	• **deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]
	• **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]
	Example:
	`Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255`
	or
	`Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0`
		In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.
		• **host** *source*—A source and source wildcard of *source* 0.0.0.0.
		• **any**—A source and source wildcard of 0.0.0.0 255.255.255.255.

Step 5	**end** **Example:** `Device(config-std-nacl)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Creating Extended Named ACLs (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** window, enter the following parameters.

- **ACL Name:** Enter the name for the ACL.
- **ACL Type:** IPv4 Extended.
- **Sequence:** Enter the sequence number.
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
- **Protocol:** Choose a protocol from the drop-down list.
- **Log:** Enable or disable logging.
- **DSCP:** Enter to match packets with the DSCP value

Step 4 Click **Add**.

Step 5 Add the rest of the rules and click **Apply to Device**.

Creating Extended Named ACLs

Follow the procedure given below to create an extended ACL using names:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended 150`	Defines an extended IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 100 to 199.
Step 4	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] **Example:** `Device(config-ext-nacl)# permit 0 any any`	In access-list configuration mode, specify the conditions allowed or denied. Use the **log** keyword to get access list logging messages, including violations. • **host** *source*—A source and source wildcard of *source* 0.0.0.0. • **host** *destintation*—A destination and destination wildcard of *destination* 0.0.0.0. • **any**—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.
Step 5	**end** **Example:** `Device(config-ext-nacl)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

When you are creating extended ACLs, remember that, by default, the end of the ACL contains an implicit deny statement for everything if it did not find a match before reaching the end. For standard ACLs, if you omit the mask from an associated IP host address access list specification, 0.0.0.0 is assumed to be the mask.

After you create an ACL, any additions are placed at the end of the list. You cannot selectively add ACL entries to a specific ACL. However, you can use **no permit** and **no deny** access-list configuration mode commands to remove entries from a named ACL.

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.

What to do next

After creating a named ACL, you can apply it to interfaces or to VLANs.

Applying an IPv4 ACL to an Interface (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Associating Interfaces**.

Step 3 Choose the interface from the **Available Interfaces** list to view its ACL details on the right-hand side. You can change the ACL details, if required.

Step 4 Click **Save & Apply to Device**.

Applying an IPv4 ACL to an Interface (CLI)

This section describes how to apply IPv4 ACLs to network interfaces.

Beginning in privileged EXEC mode, follow the procedure given below to control access to an interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Device(config)#`	Identifies a specific interface for configuration, and enter interface configuration mode. The interface can be a Layer 2 interface (port ACL), or a Layer 3 interface (router ACL).
Step 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**} **Example:** `Device(config-if)# ip access-group 2 in`	Controls access to the specified interface.
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	
Step 5	**show running-config** **Example:** `Device# show running-config`	Displays the access list configuration.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Applying ACL to Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click **Add**.

Step 3 In the **Add Policy Profile** window, click **Access Policies** tab.

Step 4 In the **WLAN ACL** area, choose the IPv4 ACL from the **IPv4 ACL** drop-down list.

Step 5 Click **Apply to Device**.

Applying ACL to Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy profile-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**ipv4 acl** *acl-name* **Example:** `Device(config-wireless-policy)# ipv4 acl test-acl`	Configures an IPv4 ACL.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuration Examples for ACLs

Examples: Including Comments in ACLs

You can use the **remark** keyword to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

To include a comment for IP numbered standard or extended ACLs, use the **access-list** *access-list number* **remark** *remark* global configuration command. To remove the remark, use the **no** form of this command.

In this example, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```
Device(config)# access-list 1 remark Permit only Jones workstation through
Device(config)# access-list 1 permit 171.69.2.88
Device(config)# access-list 1 remark Do not allow Smith through
Device(config)# access-list 1 deny 171.69.3.13
```

For an entry in a named IP ACL, use the **remark** access-list configuration command. To remove the remark, use the **no** form of this command.

In this example, the Jones subnet is not allowed to use outbound Telnet:

```
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Device(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

Examples: Applying an IPv4 ACL to a Policy Profile in a Wireless Environment

This example shows how to apply an IPv4 ACL to a Policy Profile in a Wireless environment.

Note All IPv4 ACLs must be associated to a policy profile.

This example uses extended ACLs to permit TCP traffic.

1. Creating an IPv4 ACL.

```
Device(config)# ip access-list extended <acl-name>
Device(config-ext-nacl)# 10 permit ip any 10.193.48.224 0.0.0.31
Device (config-ext-nacl)# 20 permit ip any any
```

2. Applying the IPv4 ACL to a policy profile.

```
Device(config)# wireless profile policy <policy-profile-name>
Device(config-wireless-policy)# shutdown
Device(config-wireless-policy)# ipv4 acl <acl-name>
Device(config-wireless-policy)# no shutdown
```

IPv4 ACL Configuration Examples

This section provides examples of configuring and applying IPv4 ACLs. For detailed information about compiling ACLs, see the *Cisco IOS Security Configuration Guide, Release 12.4* and to the Configuring IP Services" section in the "IP Addressing and Services" chapter of the *Cisco IOS IP Configuration Guide, Release 12.4.*

ACLs in a Small Networked Office

Figure 38: Using Router ACLs to Control Traffic



This shows a small networked office environment with routed Port 2 connected to Server A, containing benefits and other information that all employees can access, and routed Port 1 connected to Server B, containing confidential payroll data. All users can access Server A, but Server B has restricted access.

Use router ACLs to do this in one of two ways:

- Create a standard ACL, and filter traffic coming to the server from Port 1.
- Create an extended ACL, and filter traffic coming from the server into Port 1.

Examples: ACLs in a Small Networked Office

This example uses a standard ACL to filter traffic coming into Server B from a port, permitting traffic only from Accounting's source addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic coming out of routed Port 1 from the specified source address.

```
Device(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Device(config)# end
Device# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 6 out
```

This example uses an extended ACL to filter traffic coming from Server B into a port, permitting traffic from any source address (in this case Server B) to only the Accounting destination addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic going into routed Port 1, permitting it to go only to the specified destination addresses. Note that with extended ACLs, you must enter the protocol (IP) before the source and destination information.

```
Device(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Device(config)# end
Device# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 106 in
```

Example: Numbered ACLs

In this example, network 10.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 10.0.0.0 address specify a particular host. Using access list 2, the switch accepts one address on subnet 48 and reject all others on that subnet. The last line of the list shows that the switch accepts addresses on all other network 10.0.0.0 subnets. The ACL is applied to packets entering a port.

```
Device(config)# access-list 2 permit 10.48.0.3
Device(config)# access-list 2 deny 10.48.0.0 0.0.255.255
Device(config)# access-list 2 permit 10.0.0.0 0.255.255.255
Device(config)#
Device(config-if)# ip access-group 2 in
```

Examples: Extended ACLs

In this example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third line permits incoming ICMP messages for error feedback.

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Device(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Device(config)# access-list 102 permit icmp any any
Device(config)#
Device(config-if)# ip access-group 102 in
```

In this example, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Because the secure system of the network always accepts mail connections on port 25, the incoming are separately controlled.

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Device(config)#
Device(config-if)# ip access-group 102 in
```

Examples: Named ACLs

Creating named standard and extended ACLs

This example creates a standard ACL named *internet_filter* and an extended ACL named *marketing_group*. The *internet_filter* ACL allows all traffic from the source address 1.2.3.4.

```
Device(config)# ip access-list standard Internet_filter
Device(config-ext-nacl)# permit 1.2.3.4
Device(config-ext-nacl)# exit
```

The *marketing_group* ACL allows any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denies any other TCP traffic. It permits ICMP traffic, denies UDP traffic from any source to the destination address range 171.69.0.0 through 179.69.255.255 with a destination port less than 1024, denies any other IP traffic, and provides a log of the result.

```
Device(config)# ip access-list extended marketing_group
Device(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Device(config-ext-nacl)# deny tcp any any
Device(config-ext-nacl)# permit icmp any any
Device(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Device(config-ext-nacl)# deny ip any any log
Device(config-ext-nacl)# exit
```

The *Internet_filter* ACL is applied to outgoing traffic and the *marketing_group* ACL is applied to incoming traffic on a Layer 3 port.

```
Device(config)# interface gigabitethernet3/0/1

Device(config-if)# ip address 2.0.5.1 255.255.255.0
Device(config-if)# ip access-group Internet_filter out
Device(config-if)# ip access-group marketing_group in
```

Deleting individual ACEs from named ACLs

This example shows how you can delete individual ACEs from the named access list *border-list*:

```
Device(config)# ip access-list extended border-list
Device(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

Monitoring IPv4 ACLs

You can monitor IPv4 ACLs by displaying the ACLs that are configured on the switch, and displaying the ACLs that have been applied to interfaces and VLANs.

When you use the **ip access-group** interface configuration command to apply ACLs to a Layer 2 or 3 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in this table to display this information.

Table 76: Commands for Displaying Access Lists and Access Groups

Command	Purpose
show access-lists [*number* | *name*]	Displays the contents of one or all current IP and MAC address a specific access list (numbered or named).
show ip access-lists [*number* | *name*]	Displays the contents of all current IP access lists or a specific I (numbered or named).
show ip interface *interface-id*	Displays detailed configuration and status of an interface. If IP i the interface and ACLs have been applied by using the **ip access-g** configuration command, the access groups are included in the d
show running-config [**interface** *interface-id*]	Displays the contents of the configuration file for the switch or t interface, including all configured MAC and IP access lists and groups are applied to an interface.



CHAPTER 99

Downloadable ACL

- Feature History for Downloadable ACL, on page 1123
- Information About Downloadable ACL, on page 1124
- Guidelines and Restrictions for Downloadable ACL, on page 1124
- Configuring dACL Name and Definition in Cisco ISE, on page 1125
- Configuring dACL in a Controller (CLI), on page 1125
- Configuring Explicit Authorization Server List (CLI), on page 1126
- Verifying dACL Configuration, on page 1127

Feature History for Downloadable ACL

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 77: Feature History for Downloadable ACL

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Downloadable ACL	The Downloadable ACL (dACL) feature defines and updates access control lists (ACLs) in one place (Cisco ISE) and allows ACL download to all the applicable controllers. In Cisco IOS-XE 17.8 and earlier releases, you had to configure the name in Cisco ISE and define the ACL individually in each of the controllers. The dACL feature is supported only in a centralized controller with Local mode Access Points. **Note** The dACL feature is not supported in RLAN environments.

Information About Downloadable ACL

ACLs are used to restrict network access to some users or devices based on predefined criteria. These criteria are specified as a list of Access Control Entries (ACEs).

Each ACE has a matching condition based on packet header fields as follows:

- IP addresses
- ports
- protocols
- combination of IP addresses, ports, and protocols
- Result (permit or deny)

ACLs are applied to a controller on a per wireless client basis. Typically, you can configure ACLs in a controller itself. However, you can also configure ACLs to a connected Cisco ISE server and download them to the controller when a wireless client joins. Such ACLs are referred to as downloadable ACLs, per-user Dynamic ACLs, or dACLs.

Downloadable ACLs are easy to maintain because they define or update ACLs in Cisco ISE and can be downloaded to all the applicable controllers. (In Cisco IOS-XE 17.8 and earlier releases, you had to configure the name in Cisco ISE and define the ACL individually in each of the controllers.)

Scale Considerations for Downloadable ACL

The following table provides the ACL scale numbers for controllers.

Table 78: ACL Scale for Controllers

Controllers	ACL Scale
Cisco Catalyst 9800-40 Wireless Controller (small or medium)	Supports 128 ACLs with 128 ACEs.
Cisco Catalyst 9800-80 Wireless Controller (large)	Supports 256 ACLs and 256 ACEs.

Guidelines and Restrictions for Downloadable ACL

- dACL does not support FlexConnect local switching.
- IPv6 dACLs are supported only in Cisco ISE 3.0 or a later release.
- The dACL feature is supported only in a centralized controller with Local mode Access Points.

Note The dACL feature is not supported in RLAN environments.

Configuring dACL Name and Definition in Cisco ISE

Before you configure a dACL in a controller, you must configure the dACL name and definition in Cisco ISE. For more information, see Configure Per-User Dynamic Access Control Lists in ISE.

Configuring dACL in a Controller (CLI)

Before you begin

- You should have configured the RADIUS server.
- You should have configured the **aaa-override** command in the policy profile. For more information, see **Configuring AAA for Local Authentication (CLI)**.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy named-policy-profile_4`	Configures the wireless profile policy.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply policies coming from the Cisco ISE servers.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Configuring Explicit Authorization Server List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER2`	Specifies the RADIUS server name.
Step 3	**address ipv4** *ip-address* **Example:** `Device(config-radius-server)# address ipv4 124.3.52.62`	Specifies the RADIUS server parameters.
Step 4	**pac key** *key* **Example:** `Device(config-radius-server)# pack key cisco`	Specify the authorization and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 5	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 6	**aaa group server radius** *server-group-name* **Example:** `Device(config)# aaa group server radius authz-server-group`	Creates a radius server-group identification. **Note** *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.
Step 7	**aaa authorization network** *authorization-list* **group** *server-group-name* **Example:** `Device(config)# aaa authorization network authZlist group authz-server-group`	Creates an authorization method list for web-based authorization. **Note** You must use the already created authorization method list.
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying dACL Configuration

To verify the dACL, use the following command:

```
Device# show wireless client mac-address <client_mac> detail
Local Policies:
   Service Template : wlan_svc_named-policy-profile_1_local (priority 254)
    VLAN             : 16
    Absolute-Timer   : 1800
  Server Policies:
    ACS ACL          : xACSACLx-IP-tftpv4_2-62de6299
    ACS ACL          : xACSACLx-IPV6-tftpv6_2-62de8087
  Resultant Policies:
    ACS ACL          : xACSACLx-IP-tftpv4_2-62de6299
    ACS ACL          : xACSACLx-IPV6-tftpv6_2-62de8087
    VLAN Name        : VLAN0016
    VLAN             : 16
    Absolute-Timer   : 1800
```

To verify dACLs, use the following commands:

```
Device# show ip access-lists xACSACLx-IP-tftpv4_2-62de6299
Extended IP access list xACSACLx-IP-tftpv4_2-62de6299
    1 deny ip any host 9.8.29.13
    2 permit ip any any (58 matches)
```

```
Device# show ipv6 access-list xACSACLx-IPV6-tftpv6_2-62de8087
IPv6 access list xACSACLx-IPV6-tftpv6_2-62de8087
    deny ipv6 any host 2001:9:8:29:3AAD:A27A:973A:97CC sequence 1
    permit ipv6 any any (2 matches) sequence 2
```

To view all the downloaded dACLs, use the following command:

```
Device# show ip access-lists
```

CHAPTER 100

DNS-Based Access Control Lists

- Information About DNS-Based Access Control Lists, on page 1129
- Restrictions on DNS-Based Access Control Lists, on page 1132
- Flex Mode, on page 1133
- Local Mode, on page 1135
- Viewing DNS-Based Access Control Lists, on page 1139
- Configuration Examples for DNS-Based Access Control Lists, on page 1139
- Verifying DNS Snoop Agent (DSA), on page 1140
- Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL, on page 1141
- Enabling Pre-Authentication ACL for LWA and EWA (GUI), on page 1142
- Enabling Pre-Authentication ACL for LWA and EWA, on page 1143
- Enabling Post-Authentication ACL for LWA and EWA (GUI), on page 1144
- Enabling Post-Authentication ACL for LWA and EWA, on page 1145
- Enabling DNS ACL for LWA and EWA (GUI), on page 1145
- Enabling DNS ACL for LWA and EWA, on page 1145
- Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL, on page 1146

Information About DNS-Based Access Control Lists

The DNS-based ACLs are used for wireless client devices. When using these devices, you can set pre-authentication ACLs on the Cisco Catalyst 9800 Series Wireless Controller to determine the data requests that are allowed or blocked.

To enable DNS-based ACLs on the controller , you need to configure the allowed URLs or denied URLs for the ACLs. The URLs need to be pre-configured on the ACL.

With DNS-based ACLs, the client when in registration phase is allowed to connect to the configured URLs. The controller is configured with the ACL name that is returned by the AAA server. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection.

At the client authentication phase, the AAA server returns the pre-authentication ACL (url-redirect-acl, which is the attribute name given to the AAA server). The DNS snooping is performed on the AP for each client until the registration is complete and the client is in SUPPLICANT PROVISIONING state. When the ACL configured with the URLs is received on the controller , the CAPWAP payload is sent to the AP enabling DNS snooping for the URLs to be snooped.

With URL snooping in place, the AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is sent to the controller as a CAPWAP payload. The controller adds the IP address to the allowed list of IP addresses and thus the client can access the URLs configured.

URL filtering allows access to the IP address for DNS ports 80 or 443.

During pre-authentication or post-authentication, DNS ACL is applied to the client in the access point. If the client roams from one AP to another AP, the DNS learned IP addresses on the old AP is valid on the new AP as well.

Note Standard URL filtering is used for local mode, whereas enhanced URL filtering is used for flex mode local switching.

Note URL filter needs to be attached to a policy profile in case of the local mode. In the flex mode, the URL filter is attached to the flex profile and it is not need to be attached to a policy profile.

Note DNS based URLs work with active DNS query from the client. Hence, for URL filtering, the DNS should be setup correctly.

Note URL filter takes precedence over punt or redirect ACL, and over custom or static pre-auth ACL.s

Defining ACLs

Extended ACLs are like standard ACLs but identifies the traffic more precisely.

The following CLI allows you to define ACLs by name or by an identification number.

```
Device(config)#ip access-list extended ?
<100-199> Extended IP access-list number
<2000-2699> Extended IP access-list number (expanded range)
WORD Access-list name
```

The following is the structure of a CLI ACL statement:

```
<sequence number> [permit/deny] <protocol> <address or any> eq <port number> <subnet>
<wildcard>
```

For example:

```
1 permit tcp any eq www 192.168.1.0 0.0.0.255
```

The sequence number specifies where to insert the Access Control list Entry (ACE) in the ACL order of ACEs. You can define your statements with sequences of 10, 20, 30, 40, and so on.

The controller GUI allows you to write a complete ACL going to the **Configuration** > **Security** > **ACL** page. You can view a list of protocols to pick from, and make changes to an existing ACL.

Applying ACLs

The following are the ways to apply ACLs:

- **Security ACL**: A security ACL defines the type of traffic that should be allowed through the device and that which should be blocked or dropped.

  A security ACL is applied:

  - **On SVI interfaces**: The ACL will only be evaluated against the traffic that is routed through the interface.

    ```
    Device(config)# interface Vlan<number>
    Device(config-if)# ip access-group myACL in/out
    ```

  - **On a physical interface of the controller**: The ACL will be evaluated against all traffic that passes through the interface. Along with applying ACLs on SVI, this is another option for restricting traffic on the controller management plane.

    ```
    Device(config)#interface GigabitEthernet1
    Device(config-if)#ip access-group myACL in/out
    ```

  - **In the wireless policy profile or WLAN**: This option includes several places where you can configure an ACL that will be applied to the wireless client traffic, in case of central switching or local switching of traffic. Such ACLs are only supported in the inbound direction.

  - **On the AP**: In case of FlexConnect local switching, the ACL is configured and applied from the policy profile on the controller. This ACL has to be downloaded on to the AP through the Flex profile. ACLs must be downloaded to the AP before they can be applied. As an exception, fabric mode APs (in case of Software Defined Access) also use Flex ACLs even though the AP is not operating in Flex mode.

- **Punt ACL or Redirect ACL**: Punt ACL or redirect ACL refers to an ACL that specifies as to which traffic will be sent to the CPU (instead of its normal expected handling by the dataplane) for further processing. For example, the Central Web Authentication (CWA) redirect ACL defines as to which traffic is intercepted and redirected to the web login portal. The ACL does not define any traffic to be dropped or allowed, but follows the regular processing or forwarding rules, and what will be sent to the CPU for interception.

  A redirect ACL has an invisible last statement which is an implicit deny. This implicit deny is applied as a security access list entry (and therefore drops traffic that is not explicitly allowed through or sent to the CPU).

Types of URL Filters

The following are the two types of URL filters:

- **Standard**: Standard URL filters can be applied before client authentication (pre-auth) or after a successful client authentication (post-auth). Pre-auth filters are extremely useful in the case of external web authentication to allow access to the external login page, as well as, some internal websites before authentication takes place. Post-auth, they can work to block specific websites or allow only specific websites while all the rest is blocked by default. This type of URL filtering post-auth is better handled by using Cisco DNS Layer Security (formerly known as Umbrella) for more flexibility. The standard URL filters apply the same action (permit or deny) for the whole list of URLs. It is either all permit or all deny. Standard URL filter work on local mode APs only.

- **Enhanced**: Enhanced URL filters allow specification of a different action (deny or permit) for each URL inside the list and have per-URL hit counters. Enhanced URL filter work on FlexConnect mode APs only.

In both types of URL filters, you can use a wildcard sub-domain such as `*.cisco.com`. URLfilters are standalone but always applied along with an IP-based ACL. A maximum of 20 URLs are supported in a given URL filter. Considering one URL can resolve multiple IP addresses, only up to 40 resolved IP addresses can be tracked for each client. Only DNS records are tracked by URL filters. The controller or APs do not track the resolved IP address of a URL if the DNS answer uses a CNAME alias record.

Note In a scenario where you have a URL filter of type POST and an ACL applied to a policy profile, traffic to the URL is blocked by the ACL if there are no permit statements regarding the URLs. This can occur if the URL filter is POST with permit statement and within the ACL there is no permit statement for the URLs. Therefore, we recommend that you create permit statements within the ACL, regarding the IP address of the URLs, instead of using the POST URL filter.

Restrictions on DNS-Based Access Control Lists

The restriction for DNS-based ACLs is as follows:

- Pre-authentication and Post-authentication filters are supported in local modes. Only Pre-authentication filter is supported in Flex (Fabric) mode.
- ACL override pushed from ISE is not supported.
- FlexConnect Local Switching with External Web authentication using URL filtering is not supported until Cisco IOS XE Gibraltar 16.12.x.
- Fully qualified domain name (FQDN) or DNS based ACLs are not supported on Cisco Wave 1 Access Points.
- The URL filter considers only the first 20 URLs, though you can add more.
- The URL filter employs regular regex patterns and permits wildcard characters only at the beginning or at the end of an URL.
- The URL ACLs are defined and added to the FlexConnect policy profile in which they associate with a WLAN. The URL ACL creation follows a similar mechanism as that of local mode URL ACLs.
- In FlexConnect mode, the URL domain ACL works only if they are connected to a FlexConnect policy profile.
- The ACL can be attached to a WLAN by associating a policy profile with a WLAN or local policies. However, you can override it using "url-redirect-acl".
- For the Cisco AV pair received from ISE, the policy that needs to be applied for a particular client is pushed as part of ADD MOBILE

  message.
- When an AP joins or when an existing URL ACL is modified and applied on FlexConnect profile, the ACL definition along with mapped URL filter list is pushed to the AP.

- The AP stores the URL ACL definition with mapped ACL name and snoops the DNS packets for learning the first IP address for each URL in the ACL. When the AP learns the IP addresses, it updates the controller of the URL and IP bindings. The controller records this information in the client database for future use.
- When a client roams to another AP during the pre-authentication state, the learned IP addresses are pushed to a new AP. Otherwise, these learned IP addresses are purged when a client moves to a post-authentication state or when the TTL for the learned IP address expires.

Restrictions on Wildcard Support in URLs

- The generic wildcard URL, such as ***.*** is not allowed.
- Wildcard between the domain names, such as ***a.cisco.com**, **a.cisco*.com**, **a.b.c.test*.apply.play** are not allowed.
- Multiple wildcard, such as **test.*.cisco.*.com** is not allowed in a URL.
- The wildcard such as ***.cisco.com** is allowed in the URL.
- The wildcard with a suffix such as **wpr.cisco.*** is a valid configuration.
- A maximum of 16 wildcard-based URLs must be configured for a given ACL.

Flex Mode

Defining URL Filter List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter enhanced-list** *list-name* **Example:** `Device(config)# urlfilter enhanced-list urllist_flex_preauth`	Configures the URL filter enhanced list. Here, *list-name* refers to the URL filter list name. The list name must not exceed 32 alphanumeric characters.
Step 3	**url** *url-name* **preference** *0-65535* **action** {**deny** | **permit**} **Example:** `Device(config-urlfilter-enhanced-params)# url url-name preference 1 action permit`	Configures the action: permit (allowed list) or deny (blocked list).
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-urlfilter-params)# end`	

Applying URL Filter List to Flex Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *default-flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy. The default flex profile name is *default-flex-profile*.
Step 3	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy acl_name`	Configures ACL policy.
Step 4	**urlfilter list** *name* **Example:** `Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth`	Applies the URL list to the Flex profile.
Step 5	**end** **Example:** `Device(config-wireless-flex-profile-acl)# end`	Returns to privileged EXEC mode.

Configuring ISE for Central Web Authentication (GUI)

Perform the following steps to configure ISE for Central Web Authentication.

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).

Step 2 Click **Policy** and then click **Policy Elements**.

Step 3 Click **Results**.

Step 4 Expand **Authorization** and click **Authorization Profiles**.

Step 5 Click **Add** to create a new authorization profile for URL filter.

Step 6 Enter a name for the profile in the **Name** field. For example, CentralWebauth.

Step 7 Choose **ACCESS_ACCEPT** option from the **Access Type** drop-down list.

Step 8 Alternatively, in the **Common Tasks** section, check **Web Redirection**..

Step 9 Choose the **Centralized Web Auth** option from the drop-down list.

Step 10 Specify the ACL and choose the ACL value from the drop-down list.

Step 11 In the **Advanced Attributes Setting** section, choose **Cisco:cisco-av-pair** from the drop-down list.

Note Multiple ACL can be applied on the controller based on priority. In L2 Auth + webauth multi-auth scenario, if the ISE returns ACL during L2 Auth then ISE ACL takes precedence over the default webauth redirect ACL. This leads to traffic running in webauth pending state, if ISE ACL has permit rule. To avoid this scenario, you need to set the precedence for L2 Auth ISE returned ACL. The default webauth redirect ACL priority is 100. To avoid traffic issue, you need to configure the redirect ACL priority above 100 for ACL returned by ISE.

Step 12 Enter the following one by one and click (+) icon after each of them:

- url-redirect-acl=<sample_name>
- url-redirect=<sample_redirect_URL>

  For example,

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?
sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-005056bf2f0a&daysToExpiry=value&action=cwa
```

Step 13 Verify contents in the **Attributes Details** section and click **Save**.

Local Mode

Defining URL Filter List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter list** *list-name* **Example:** `Device(config)# urlfilter list urllist_local_preauth`	Configures the URL filter list. Here, *list-name* refers to the URL filter list name. The list name must not exceed 32 alphanumeric characters.

	Command or Action	Purpose
Step 3	**action permit** **Example:** `Device(config-urlfilter-params)# action permit`	Configures the action: permit (allowed list) or deny (blocked list).
Step 4	**filter-type post-authentication** **Example:** `Device(config-urlfilter-params)# filter-type post-authentication`	**Note** This step is applicable while configuring post-authentication URL filter only. Configures the URL list as post-authentication filter.
Step 5	**redirect-server-ip4** *IPv4-address* **Example:** `Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101`	Configures the IPv4 redirect server for the URL list. Here, *IPv4-address* refers to the IPv4 address.
Step 6	**redirect-server-ip6** *IPv6-address* **Example:** `Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82`	Configures the IPv6 redirect server for the URL list. Here, *IPv6-address* refers to the IPv6 address.
Step 7	**url** *url* **Example:** `Device(config-urlfilter-params)# url url1.dns.com`	Configures an URL. Here, *url* refers to the name of the URL.
Step 8	**end** **Example:** `Device(config-urlfilter-params)# end`	Returns to privileged EXEC mode.

Applying URL Filter List to Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click on the **Policy Name**.

Step 3 Go to **Access Policies** tab.

Step 4 In the **URL Filters** section, choose the filters from the **Pre Auth** and **Post Auth** drop-down lists.

Step 5 Click **Update & Apply to Device**.

Applying URL Filter List to Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures wireless policy profile. Here, *profile-policy* refers to the name of the WLAN policy profile.

Step 3	**urlfilter list** {**pre-auth-filter** *name* | **post-auth-filter** *name*}
	Example:
	`Device(config-wireless-policy)# urlfilter list pre-auth-filter urllist_local_preauth`
	`Device(config-wireless-policy)# urlfilter list post-auth-filter urllist_local_postauth`
		Applies the URL list to the policy profile.
		Here, *name* refers to the name of the pre-authentication or post-authentication URL filter list configured earlier.
		Note During the client join, the URL filter configured on the policy will be applied.

Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Configuring ISE for Central Web Authentication

Creating Authorization Profiles

Procedure

Step 1 Login to the Cisco Identity Services Engine (ISE).
Step 2 Click **Policy**, and click **Policy Elements**.
Step 3 Click **Results**.
Step 4 Expand **Authorization**, and click **Authorization Profiles**.
Step 5 Click **Add** to create a new authorization profile for URL filter.
Step 6 In the Name field, enter a name for the profile. For example, *CentralWebauth*.
Step 7 Choose **ACCESS_ACCEPT** from the Access Type drop-down list.
Step 8 In the Advanced Attributes Setting section, choose **Cisco:cisco-av-pair** from the drop-down list.
Step 9 Enter the following one by one and click (+) icon after each of them:

- url-filter-preauth=<preauth_filter_name>
- url-filter-postauth=<postauth_filter_name>

For example,

```
Cisco:cisco-av-pair = url-filter-preauth=urllist_pre_cwa
Cisco:cisco-av-pair = url-filter-postauth=urllist_post_cwa
```

Step 10 Verify contents in the Attributes Details section and click **Save**.

Mapping Authorization Profiles to Authentication Rule

Procedure

Step 1 In the **Policy** > **Authentication** page, click **Authentication**.

Step 2 Enter a name for your authentication rule.

For example, *MAB*.

Step 3 In the If condition field, select the plus (+) icon.

Step 4 Choose **Compound condition**, and choose **WLC_Web_Authentication**.

Step 5 Click the arrow located next to **and ...** in order to expand the rule further.

Step 6 Click the + icon in the Identity Source field, and choose **Internal endpoints**.

Step 7 Choose **Continue** from the 'If user not found' drop-down list.

This option allows a device to be authenticated even if its MAC address is not known.

Step 8 Click **Save**.

Mapping Authorization Profiles to Authorization Rule

Procedure

Step 1 Click **Policy** > **Authorization**.

Step 2 In the Rule Name field, enter a name.

For example, *CWA Post Auth*.

Step 3 In the Conditions field, select the plus (+) icon.

Step 4 Click the drop-down list to view the Identity Groups area.

Step 5 Choose **User Identity Groups** > **user_group**.

Step 6 Click the plus (+) sign located next to **and ...** in order to expand the rule further.

Step 7 In the Conditions field, select the plus (+) icon.

Step 8 Choose **Compound Conditions**, and choose to create a new condition.

Step 9 From the settings icon, select **Add Attribute/Value** from the options.

Step 10 In the Description field, choose **Network Access** > **UseCase** as the attribute from the drop-down list.

Step 11 Choose the **Equals** operator.

Step 12 From the right-hand field, choose **GuestFlow**.

Step 13 In the Permissions field, select the plus (+) icon to select a result for your rule.

You can choose **Standard** > **PermitAccess** option or create a custom profile to return the attributes that you like.

Viewing DNS-Based Access Control Lists

To view details of a specified wireless URL filter, use the following command:

```
Device# show wireless urlfilter details <urllist_flex_preauth>
```

To view the summary of all wireless URL filters, use the following command:

```
Device# show wireless urlfilter summary
```

To view the URL filter applied to the client in the resultant policy section, use the following command:

```
Device# show wireless client mac-address <MAC_addr> detail
```

Configuration Examples for DNS-Based Access Control Lists

Flex Mode

Example: Defining URL Filter List

This example shows how to define URL list in Flex mode:

```
Device# configure terminal
Device(config)# urlfilter enhanced-list urllist_flex_pre
Device(config-urlfilter-params)# url www.dns.com preference 1 action permit
Device(config-urlfilter-params)# end
```

Example: Applying URL Filter List to Flex Profile

This example shows how to apply an URL list to the Flex profile in Flex mode:

```
Device# configure terminal
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy acl_name
Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth
Device(config-wireless-flex-profile-acl)# end
```

Local Mode

Example: Defining Preauth URL Filter List

This example shows how to define URL filter list (pre-authentication):

```
Device# configure terminal
Device(config)# urlfilter list urllist_local_preauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

Example: Defining Postauth URL Filter List

This example shows how to define URL filter list (post-authentication):

```
Device# configure terminal
Device(config)# urlfilter list urllist_local_postauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# filter-type post-authentication
Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

Example: Applying URL Filter List to Policy Profile

This example shows how to apply an URL list to the policy profile in local mode:

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# urlfilter list pre-auth-filter urllist_local_preauth
Device(config-wireless-policy)# urlfilter list post-auth-filter urllist_local_postauth
Device(config-wireless-policy)# end
```

Verifying DNS Snoop Agent (DSA)

To view details of the DNS snooping agent client, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
```

To view details of the DSA enabled interface, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf
```

To view the pattern list in uCode memory, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list
```

To view the OpenDNS string for the pattern list, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list odns_string
```

To view the FQDN filter for the pattern list, use the following command:

```
Device#
show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list
fqdn-filter <fqdn_filter_ID>
```

Note The valid range of *fqdn_filter_ID* is from 1 to 16.

To view details of the DSA client, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client info
```

To view the pattern list in CPP client, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list
```

To view the OpenDNS string for the pattern list, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list
 odns_string
```

To view the FQDN filter for the pattern list, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list
 fqdn-filter <fqdn_filter_ID>
```

Note The valid range of *fqdn_filter_ID* is from 1 to 16.

To view details of the DSA datapath, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
```

To view details of the DSA IP cache table, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
```

To view details of the DSA address entry, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 address {ipv4 <IPv4_addr> | ipv6 <IPv6_addr>}
```

To view details of all the DSA IP cache address, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 all
```

To view details of the DSA IP cache pattern, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 pattern <pattern>
```

To view details of the DSA datapath memory, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath memory
```

To view the DSA regular expression table, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
regexp-table
```

To view the DSA statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath stats
```

Information About Flex Client IPv6 Support with WebAuth Pre and Post ACL

IOS IPv6 ACLs is used to send webauth ACL to an AP. A change in the ACL policies of the Flex profile (new ACL, deleted ACL or modified ACL).

ACL definitions are pushed to AP in the following events:

- AP join.
- New ACL mapping in a new Flex profile.
- Configuring IPv6 ACL definition in Flex profile.

Default Local Web Authentication ACLs

The pre-defined default LWA IPv6 ACL is pushed to AP and plumbed to data plane.

Default External Web Authentication ACL

The default EWA ACLs are derived from the redirect portal address configured in the parameter map.

The following list covers the types of default EWA ACLs:

- Security ACL—Pushed and plumbed to AP.
- Intercept ACL—Pushed and plumbed to data plane.

FQDN ACL

- FQDN ACL is encoded along with IPv6 ACL and sent to AP.
- FQDN ACL is always a custom ACL.

The following applies to Flex and Local mode:

- If you are migrating from AireOS, you would explicitly need to execute the following commands:

```
redirect append ap-mac tag ap_mac
redirect append wlan-ssid tag wlan
redirect append client-mac tag client_mac
```

- If the login page has any resource that needs to be fetched from the server, you will need to include those resource URLs in URL filtering.
- If you are trying to access IPv6 URL and you have an IPv4 web server, the controller redirects the client to an internal page as domain redirection is not supported. It is recommended to have a dual-stack web server and configure virtual IPv6 address in the global parameter map.

Enabling Pre-Authentication ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Uncheck the **WPAPolicy**, **AES** and **802.1x** check boxes.

Step 5 Choose **Security** > **Layer3** tab. Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and authentication list from the **Authentication List** drop-down list. Click **Show Advanced Settings** and under the **Preauthenticated ACL** settings, choose the IPv6 ACL from the **IPv6** drop-down list.

Step 6 Choose **Security** > **AAA** tab. Choose the authentication list from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Enabling Pre-Authentication ACL for LWA and EWA

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Enters the WLAN configuration sub-mode. • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** If you have already configured WLAN, enter **wlan wlan-name** command.
Step 3	**ipv6 traffic-filter web** *acl_name-preauth* **Example:** `Device(config-wlan)# ipv6 traffic-filter web preauth_v6_acl`	Creates a pre-authentication ACL for web authentication.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables the WPA security.
Step 5	**no security wpa wpa2 ciphers aes** **Example:**	Disables WPA2 ciphers for AES.

	Command or Action	Purpose
	`Device(config-wlan)#no security wpa wpa2 ciphers aes`	
Step 6	**no security wpa akm dot1x** **Example:** `Device(config-wlan)#no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 7	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Configures web authentication.
Step 8	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list wcm_dot1x`	Enables authentication list for WLAN.
Step 9	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map param-custom-webconsent`	Maps the parameter map.
Step 10	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Shutdown the WLAN.

Enabling Post-Authentication ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**. The **Profile Name** is the profile name of the policy profile.

Step 4 Enter the **SSID** and the **WLAN ID**.

Step 5 Click **Apply to Device**.

Enabling Post-Authentication ACL for LWA and EWA

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy test1`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**ipv6 acl** *acl_name* **Example:** `Device(config-wireless-policy)# ipv6 acl testacl`	Creates a named WLAN ACL.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling DNS ACL for LWA and EWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**. The **Profile Name** is the profile name of the policy profile.

Step 4 Enter the **SSID** and the **WLAN ID**.

Step 5 Click **Apply to Device**.

Enabling DNS ACL for LWA and EWA

Note Post-authentication DNS ACL is not supported.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy test1`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Flex Client IPv6 Support with WebAuth Pre and Post ACL

To verify the client state after L2 authentication, use the following command:

```
Device# show wireless client summary
Number of Local Clients: 1


MAC Address    AP Name                           WLAN  State             Protocol Method
  Role
-------------------------------------------------------------------------------------------------
1491.82b8.f8c1 AP4001.7A03.544C                  4      Webauth Pending   11n(5)   None
   Local

Number of Excluded Clients: 0
```

To verify the IP state, discovery, and MAC, use the following command:

```
Device# show wireless dev da ip
  IP                                        STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------------------
  15.30.0.4                                 Reachable   ARP         1491.82b8.f8c1
  2001:15:30:0:d1d7:ecf3:7940:af60          Reachable   IPv6 Packet 1491.82b8.f8c1
  fe80::595e:7c29:d7c:3c84                  Reachable   IPv6 Packet 1491.82b8.f8c1
```

CHAPTER 101

Allowed List of Specific URLs

- Allowed List of Specific URLs, on page 1147
- Adding URL to Allowed List, on page 1147
- Verifying URLs on the Allowed List, on page 1149

Allowed List of Specific URLs

This feature helps you to add specific URLs to allowed list on the controller or the AP so that those specific URLs are available for use, even when there is no connectivity to the internet. You can add URLs to allowed list for web authentication of captive portal and walled garden. Authentication is not required to access the allowed list of URLs. When you try to access sites that are not in allowed list, you are redirected to the Login page.

Adding URL to Allowed List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter list** *<urlfilter-name>* **Example:** `Device(config)# urlfilter list url-allowedlist-nbn`	Configures the URL filter profile.
Step 3	**action** [**deny** | **permit**] **Example:** `Device(config-urlfilter-params)# action permit`	Configures the list as allowed list. The **permit** command configures the list as allowed list and the **deny** command configures the list as blocked list.

	Command or Action	Purpose
Step 4	{**redirect-server-ipv4** | **redirect-server-ipv6**} **Example:** `Device(config-urlfilter-params)# redirect-server-ipv4 X.X.X.X`	Configures the IP address of the redirect servers to which the user requests will be redirected in case of denied requests.
Step 5	**url** *url-to-be-allowed* **Example:** `Device(config-urlfilter-params)# url www.cisco.com`	Configures the URL to be allowed.

Note The controller uses two IP addresses and the mechanism only allows for one portal IP to be allowed. To allow pre-authentication access to more HTTP ressources, you need to use URL filters which will dynamically makes holes in the intercept (redirect) and security (preauth) ACLs for the IPs related to the website whose URL you enter in the URL filter. DNS requests will be dynamically snooped for the controller to learn the IP address of those URLs and add it to the ACLs dynamically.

Note **redirect-server-ipv4** and **redirect-server-ipv6** is applicable only in the local mode, specifically in post-authentication. For any further tracking or displaying any warning messages, the denied user request is redirected to the configured server.

But the **redirect-server-ipv4** and **redirect-server-ipv6** configurations do not apply to pre-authentication scenario as you will be redirected to the controller for the redirect login URL for any denied access.

You can associate the allowed URL with the ACL policy in flex profile.

Example

Associating the allowed URL with the ACL policy in flex profile:

```
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy user_v4_acl
Device(config-wireless-flex-profile-acl)# urlfilter list url_allowedlist_nbn
Device(config-wireless-flex-profile-acl)# exit
Device(config-wireless-flex-profile)# description "default flex profile"

Device(config)# urlfilter enhanced-list urllist_pre_cwa
Device(config-urlfilter-enhanced-params)# url url1.dns.com preference 1 action permit
Device(config-urlfilter-enhanced-params)# url url2.dns.com preference 2 action deny
Device(config-urlfilter-enhanced-params)# url url3.dns.com preference 3 action permit

Device(config)# wlan wlan5 5 wlan5
Device(config-wlan)#ip access-group web user_v4_acl
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa
Device(config-wlan)#no security wpa wpa2 ciphers aes
Device(config-wlan)#no security wpa akm dot1x
Device(config-wlan)#security web-auth
Device(config-wlan)#security web-auth authentication-list default
```

```
Device(config-wlan)#security web-auth parameter-map global
Device(config-wlan)#no shutdown
```

Verifying URLs on the Allowed List

Verify URLs on the Allowed List.

```
Device# show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                        ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
-------------------------------------------------------------------------------------------------
url-whitelist                   1    PRE-AUTH     PERMIT   1.1.1.1

Device#

Device# show wireless urlfilter details url-whitelist
List Name..................... : url-whitelist
Filter ID..................... : : 1
Filter Type................... : PRE-AUTH
Action........................ : PERMIT
Redirect server ipv4...... : 1.1.1.1
Redirect server ipv6...... :
Configured List of URLs
   URL........................ : www.cisco.com
```

CHAPTER 102

Cisco Umbrella WLAN

- Information About Cisco Umbrella WLAN, on page 1151
- Registering Controller to Cisco Umbrella Account, on page 1152
- Configuring Cisco Umbrella WLAN, on page 1153
- Configuring the Umbrella Flex Profile, on page 1159
- Configuring the Umbrella Flex Profile (GUI), on page 1159
- Configuring Umbrella Flex Parameters, on page 1160
- Configuring the Umbrella Flex Policy Profile (GUI), on page 1160
- Verifying the Cisco Umbrella Configuration, on page 1161

Information About Cisco Umbrella WLAN

The Cisco Umbrella WLAN provides a cloud-delivered network security service at the Domain Name System (DNS) level, with automatic detection of both known and emergent threats.

This feature allows you to block sites that host malware, bot networks, and phishing before they actually become malicious.

Cisco Umbrella WLAN provides the following:

- Policy configuration per user group at a single point.
- Policy configuration per network, group, user, device, or IP address.

  The following is the policy priority order:

  1. Local policy
  2. AP group
  3. WLAN

- Visual security activity dashboard in real time with aggregated reports.
- Schedule and send reports through email.
- Support up to 60 content categories, with a provision to add custom allowed list and blocked list entries.
- Supports custom parameter-type Umbrella profiles. One Global profile and 15 custom profiles are supported.

- Although IPv6 is supported, device registration will always be over IPv4. There is no support of device registration over IPv6.
- The communication from device to the Umbrella Cloud can be done over IPv6 also.
- In the Flexconnect mode, DNS handling takes place in the AP instead of the controller. Multiple profiles are supported in the Flex mode.

This feature does not work in the following scenarios:

- If an application or host use an IP address directly, instead of using DNS to query domain names.
- If a client is connected to a web proxy and does not send a DNS query to resolve the server address.

Registering Controller to Cisco Umbrella Account

Before you Begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

This section describes the process followed to register the controller to the Cisco Umbrella account.

The controller is registered to Cisco Umbrella server using the Umbrella parameter map. Each of the Umbrella parameter map must have an API token. The Cisco Umbrella responds with the device ID for the controller . The device ID has a 1:1 mapping with the Umbrella parameter map name.

Fetching API token for Controller from Cisco Umbrella Dashboard

From Cisco Umbrella dashboard, verify that your controller shows up under Device Name, along with their identities.

Applying the API Token on Controller

Registers the Cisco Umbrella API token on the network.

DNS Query and Response

Once the device is registered and Umbrella parameter map is configured on WLAN, the DNS queries from clients joining the WLAN are redirected to the Umbrella DNS resolver.

Note This is applicable for all domains not configured in the local domain RegEx parameter map.

The queries and responses are encrypted based on the DNScrypt option in the Umbrella parameter map.

For more information on the Cisco Umbrella configurations, see the Integration for ISR 4K and ISR 1100 – Security Configuration Guide.

Limitations and Considerations

The limitations and considerations for this feature are as follows:

- You will be able to apply the wireless Cisco Umbrella profiles to wireless entities, such as, WLAN or AP groups, if the device registration is successful.
- In case of L3 mobility, the Cisco Umbrella must be applied on the anchor controller always.
- When two DNS servers are configured under DHCP, two Cisco Umbrella server IPs are sent to the client from DHCP option 6. If only one DNS server is present under DHCP, only one Cisco Umbrella server IP is sent as part of DHCP option 6.

Configuring Cisco Umbrella WLAN

To configure Cisco Umbrella on the controller , perform the following:

- You must have the API token from the Cisco Umbrella dashboard.
- You must have the root certificate to establish HTTPS connection with the Cisco Umbrella registration server: api.opendns.com. You must import the root certificate from **digicert.com** to the controller using the **crypto pki trustpool import terminal** command.

Importing CA Certificate to the Trust Pool

Before you begin

The following section covers details about how to fetch the root certificate and establish HTTPS connection with the Cisco Umbrella registration server:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	Perform either of the following tasks: • **crypto pki trustpool import url** *url* `Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b` Imports the root certificate directly from the Cisco website.	

	Command or Action	Purpose

	Note The Trustpool bundle contains the root certificate of *digicert.com* together with other CA certificates.
	
	• **crypto pki trustpool import terminal**
	
	`Device(config)# crypto pki trustpool import terminal`
	
	Imports the root certificate by executing the import terminal command.
	
	• Enter PEM-formatted CA certificate from the following location: See the Related Information section to download the CA certificate.
	
	`-----BEGIN CERTIFICATE-----`
	`MIIE6jCCA9KgAwIBAgIQCjUI1VwpKwF9+K1lwA/35DANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQG`
	`EwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29tMSAw`
	`HgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBDQTAeFw0yMDA5MjQwMDAwMDBaFw0zMDA5MjMy`
	`MzU5NTlaME8xCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERp`
	`Z2lDZXJ0IFRMUyBSU0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB`
	`CgKCAQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ly5CiDt3+PE0J6aqXodgojl`
	`EVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQ9XE0w6Dohg9/n0OurTCRpt8OnRDt`
	`VIF0LuJ9xspiIhMbfyOLJWwTRYALE//i+p1hJnuWaKmxW8oHzf6VGolbDtN+I2tLJYrVU`
	`muHZ9ojRXj1hERG/cU9WLQqjGBAfr5yjK7tI4nyfFK3TLqNX3sN+roO6JWHgXjkkD`
	`Ka7SU+kEbn8lwZ2lreaonicgE7XQPUDTTAk+q9QIDAQABo4IBrjCCAaowHQYDVR0OBBYE`
	`FLdrouqoqoSMeeq02g+YssWVdrn0MB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA4G`
	`A1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwEgYDVR0TAQH/BAgw`
	`BgEB/wIBADB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0`
	`LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xv`
	`YmFsUm9vdENBLmNydDB7BgNVHR8EdDByMDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20v`
	`RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20v`
	`RGlnaUNlcnRHbG9iYWxSb290Q0EuY3JsMDAGA1UdIAQpMCcwBwYFZ4EMAQEwCAYGZ4EMAQIBMAgG`
	`BmeBDAECAjAIBgZngQwBAgMwDQYJKoZIhvcNAQELBQADggEBAHert3onPa679n/gWlbJhKrKW3EX`
	`3SJH/E6f7tDBpATho+vFScH90cnfjK+URSxGKqNjOSD5nkoklEHIqdninFQFBstcHL4AGw+oWv8Z`
	`u2XHFq8hVt1hBcnpj5h232sb0HIMULkwKXq/YFkQZhM6LawVEWwtIwwCPgU7/uWhnOKK24fXSuhe`
	`50gG66sSnvKhMNbgjOZYQrAKHCjxMbWKiKnpPMzEFMhoCw+dj20tlQj7T9rxkTgl4ZxuYRiHas6xuwAwapu3r9rxxZf+ingkquqTgLozZXq8oXfpf2kUCwA/d5KxTVtzhwoT0JzI8ks5T1KESaZMkE4f97Q=`
	`-----END CERTIFICATE-----`
	
	Imports the root certificate by pasting the CA certificate from the **digicert.com**.	

Step 3	**quit** **Example:** `Device(config)# quit`	Imports the root certificate by entering the **quit** command. **Note** You will receive a message after the certificate has been imported.

Creating a Local Domain RegEx Parameter Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type regex** *parameter-map-name* **Example:** `Device(config)# parameter-map type regex dns_wl`	Creates a regex parameter map.
Step 3	**pattern** *regex-pattern* **Example:** `Device(config-profile)# pattern www.google.com`	Configures the regex pattern to match. **Note** The following patterns are supported: • Begins with `.*`. For example: **`.*facebook.com`** • Begins with `.*` and ends with `*` . For example: **`.*google*`** • Ends with `*`. For example: **`www.facebook*`** • No special character. For example: **`www.facebook.com`**
Step 4	**end** **Example:** `Device(config-profile)# end`	Returns to privileged EXEC mode.

Configuring Parameter Map Name in WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click on the Policy Profile Name. The **Edit Policy Profile** window is displayed.

Step 3 Choose the **Advanced** tab.

Step 4 In the **Umbrella** settings, from the **Umbrella Parameter Map** drop-down list, choose the parameter map.

Step 5 Enable or disable **Flex DHCP Option for DNS** and **DNS Traffic Redirect** toggle buttons.

Step 6 Click **Update & Apply to Device**.

Configuring the Umbrella Parameter Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type umbrella global** | *parameter-map-name* **Example:** `Device(config)# parameter-map type umbrella custom_pmap`	Creates an umbrella global or customized parameter map.
Step 3	**token** *token-value* **Example:** `Device(config-profile)# token 5XXXXXXXXCXXXXXXXAXXXXXXXFXXXXCXXXXXXXX`	Configures an umbrella token.
Step 4	**local-domain** *regex-parameter-map-name* **Example:** `Device(config-profile)# local-domain dns_wl`	Configures local domain RegEx parameter map.
Step 5	**resolver** {**IPv4** *X.X.X.X* | **IPv6** *X:X:X:X::X*} **Example:** `Device(config-profile)# resolver IPv6 10:1:1:1::10`	Configures the Anycast address. The default address is applied when there is no specific address configured.
Step 6	**end** **Example:** `Device(config-profile)# end`	Returns to privileged EXEC mode.

Enabling or Disabling DNScrypt (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Threat Defence** > **Umbrella**.

Step 2 Enter the **Registration Token** received from Umbrella. Alternatively, you can click on **Click here to get your Token**to get the token from Umbrella.

Step 3 Enter the **Whitelist Domains** that you want to exclude from filtering.

Step 4 Check or uncheck the **Enable DNS Packets Encryption** check box to encrypt or decrypt the DNS packets.

Step 5 Click **Apply**.

Enabling or Disabling DNScrypt

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Creates an umbrella global parameter map.
Step 3	[**no**] **dnscrypt** **Example:** `Device(config-profile)# no dnscrypt`	Enables or disables DNScrypt. By default, the DNScrypt option is enabled. **Note** Cisco Umbrella DNScrypt is not supported when DNS-encrypted responses are sent in the data-DTLS encrypted tunnel (either mobility tunnel or AP CAPWAP tunnel).
Step 4	**end** **Example:** `Device(config-profile)# end`	Returns to privileged EXEC mode.

Configuring Timeout for UDP Sessions

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Creates an umbrella global parameter map.
Step 3	**udp-timeout** *timeout_value* **Example:** `Device(config-profile)# udp-timeout 2`	Configures timeout value for UDP sessions. The *timeout_value* ranges from 1 to 30 seconds. **Note** The **public-key** and **resolver** parameter-map options are automatically populated with the default values. So, you need not change them.
Step 4	**end** **Example:** `Device(config-profile)# end`	Returns to privileged EXEC mode.

Configuring Parameter Map Name in WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Click on the Policy Profile Name. The **Edit Policy Profile** window is displayed.
Step 3 Choose the **Advanced** tab.
Step 4 In the **Umbrella** settings, from the **Umbrella Parameter Map** drop-down list, choose the parameter map.
Step 5 Enable or disable **Flex DHCP Option for DNS** and **DNS Traffic Redirect** toggle buttons.
Step 6 Click **Update & Apply to Device**.

Configuring Parameter Map Name in WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:**	Creates policy profile for the WLAN.

	Command or Action	Purpose
	`Device(config)# wireless profile policy default-policy-profile`	The *profile-name* is the profile name of the policy profile.
Step 3	**umbrella-param-map** *umbrella-name* **Example:** `Device(config-wireless-policy)# umbrella-param-map global`	Configures the Umbrella OpenDNS feature for the WLAN.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the Umbrella Flex Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy. Enters the flex profile configuration mode. The *flex-profile-name* is the flex profile name.
Step 3	**umbrella-profile** *umbrella-profile-name* **Example:** `Device(config-wireless-flex-profile)# umbrella-profile global`	Configures the Umbrella flex feature. Use the **no** form of this command to negate the command or to set the command to its default.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the Umbrella Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click a **Flex Profile Name**. The **Edit Flex Profile** dialog box appears.

Step 3 Under the **Umbrella** tab, click the **Add** button.

Step 4 Select a name for the parameter map from the **Parameter Map Name** drop-down list and click **Save**.

Step 5 Click the **Update & Apply to Device** button. The configuration changes are successfully applied.

Configuring Umbrella Flex Parameters

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile. Enters the wireless policy profile configuration mode. The *policy-profile-name* is the WLAN policy profile name.
Step 3	**flex umbrella dhcp-dns-option** **Example:** `Device(config-wireless-policy-profile)# [no] flex umbrella dhcp-dns-option`	Configures the Umbrella DHCP option for DNS. By default the option is enabled.
Step 4	**flex umbrella mode** {**force** | **ignore**} **Example:** `Device(config-wireless-policy-profile)# [no] flex umbrella mode force`	Configures the DNS traffic to be redirected to Umbrella. You can either forcefully redirect the traffic or choose to ignore the redirected traffic to Umbrella. The default mode is **ignore**.
Step 5	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the Umbrella Flex Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Policy**.

Step 2 Click the **Add** button. The **Add Policy Profile** dialog box appears.

Step 3 In the **Advanced** tab, and under the **Umbrella** section, complete the following:

a) Select the parameter map from the **Umbrella Parameter Map** drop-down list. Click the **Clear** hyperlink to clear the selection.
b) Click the field adjacent to **Flex DHCP Option for DNS** to **Disable** the option. By default it is **Enabled**.
c) Click the field adjacent to **DNS Traffic Redirect** to set the option to **Force**. By default it is set to **Ignore**.

Step 4 Click the **Apply to Device** button.

Verifying the Cisco Umbrella Configuration

To view the Umbrella configuration details, use the following command:

```
Device# show umbrella config
Umbrella Configuration
=======================
Token: 5XXXXXXABXXXXXFXXXXXXXXXXDXXXXXXXXXXXXABXX
API-KEY: NONE
OrganizationID: xxxxxxx
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt: Not enabled
Public-key: NONE
UDP Timeout: 5 seconds
Resolver address:
1. 10.1.1.1
2. 5.5.5.5
3. XXXX:120:50::50
4. XXXX:120:30::30
```

To view the device registration details, use the following command:

```
Device# show umbrella deviceid
Device registration details
Param-Map Name                  Status          Device-id
global                          200 SUCCESS     010aa4eXXXXXXX8d
vj-1                            200 SUCCESS     01XXXXXXXf4541e1
GUEST                           200 SUCCESS     010a4f6XXXXXXX42
EMP                             200 SUCCESS     0XXXXXXXXd106ecd
```

To view the detailed description for the Umbrella device ID, use the following command:

```
Device# show umbrella deviceid detailed
Device registration details

 1.global
      Tag               : global
      Device-id         : 010aa4eXXXXXXX8d
      Description       : Device Id recieved successfully
      WAN interface     : None
 2.vj-1
      Tag               : vj-1
      Device-id         : 01XXXXXXXf4541e1
      Description       : Device Id recieved successfully
      WAN interface     : None
```

To view the Umbrella DNSCrypt details, use the following command:

```
Device# show umbrella dnscrypt
DNSCrypt: Enabled
   Public-key: B111:XXXX:XXXX:XXXX:3E2B:XXXX:XXXX:XXXE:XXX3:3XXX:DXXX:XXXX:BXXX:XXXB:XXXX:FXXX

    Certificate Update Status: In Progress
```

To view the Umbrella global parameter map details, use the following command:

```
Device# show parameter-map type umbrella global
```

To view the regex parameter map details, use the following command:

```
Device# show parameter-map type regex <parameter-map-name>
```

To view the Umbrella statistical information, use the following command:

```
Device# show platform hardware chassis active qfp feature umbrella datapath stats
```

To view the wireless policy profile Umbrella configuration, use the following command:

```
Device#show wireless profile policy detailed vj-pol-profile | s Umbrella
Umbrella information
Cisco Umbrella Parameter Map : vj-2
DHCP DNS Option : ENABLED
Mode : force
```

To view the wireless flex profile Umbrella configuration, use the following command:

```
Device#show wireless profile flex detailed vj-flex-profile | s Umbrella
Umbrella Profiles :
vj-1
vj-2
global
```

To view the Umbrella details on the AP, use the following command:

```
AP#show client opendns summary
Server-IP role
208.67.220.220 Primary
208.67.222.222 Secondary

Server-IP role
2620:119:53::53 Primary
2620:119:35::35 Secondary

Wlan Id DHCP OpenDNS Override Force Mode
0 true false
1 false false
...

15 false false
Profile-name Profile-id
vj-1 010a29b176b34108
global 010a57bf502c85d4
vj-2 010ae385ce6c1256
AP0010.10A7.1000#

Client to profile command

AP#show client opendns address 50:3e:aa:ce:50:17
Client-mac Profile-name
50:3E:AA:CE:50:17 vj-1
AP0010.10A7.1000#
```

CHAPTER 103

RADIUS Server Load Balancing

- Information About RADIUS Server Load Balancing, on page 1163
- Prerequisites for RADIUS Server Load Balancing, on page 1165
- Restrictions for RADIUS Server Load Balancing, on page 1165
- Enabling Load Balancing for a Named RADIUS Server Group (CLI), on page 1165

Information About RADIUS Server Load Balancing

RADIUS Server Load Balancing Overview

By default, if two RADIUS servers are configured in a server group, only one is used. The other server acts as standby, if the primary server is declared as dead, the secondary server receives all the load.

If you need both servers to perform transactions actively, you need to enable Load Balancing.

Note By default, load balancing is not enabled on the RADIUS server group.

If you enable load balancing in a RADIUS server group with two or more RADIUS servers, the Server A and Server B receives a AAA transaction. The transaction queues are checked in Server A and Server B. The server with less number of outstanding transactions are assigned the next batch of AAA transaction.

Load balancing distributes batches of transactions to RADIUS servers in a server group. Load balancing assigns each batch of transactions to the server with the lowest number of outstanding transactions in its queue. The process of assigning a batch of transactions is as follows:

1. The first transaction is received for a new batch.
2. All server transaction queues are checked.
3. The server with the lowest number of outstanding transactions is identified.
4. The identified server is assigned the next batch of transactions.

The batch size is a user-configured parameter. Changes in the batch size may impact CPU load and network throughput. As batch size increases, CPU load decreases, and network throughput increases. However, if a large batch size is used, all available server resources may not be fully utilized. As batch size decreases, CPU load increases and network throughput decreases.

Note There is no set number for large or small batch sizes. A batch with more than 50 transactions is considered large and a batch with fewer than 25 transactions is considered small.

Note If a server group contains ten or more servers, we recommend that you set a high batch size to reduce CPU load.

Transaction Load Balancing Across RADIUS Server Groups

You can configure load balancing either per-named RADIUS server group or for the global RADIUS server group. The load balancing server group must be referred to as "radius" in the authentication, authorization, and accounting (AAA) method lists. All public servers that are part of the RADIUS server group are then load balanced.

You can configure authentication and accounting to use the same RADIUS server or different servers. In some cases, the same server can be used for preauthentication, authentication, or accounting transactions for a session. The preferred server, which is an internal setting and is set as the default, informs AAA to use the same server for the start and stop record for a session regardless of the server cost. When using the preferred server setting, ensure that the server that is used for the initial transaction (for example, authentication), the preferred server, is part of any other server group that is used for a subsequent transaction (for example, accounting).

The preferred server is not used if one of the following criteria is true:

- The **load-balance method least-outstanding ignore-preferred-server** command is used.
- The preferred server is dead.
- The preferred server is in quarantine.
- The want server flag has been set, overriding the preferred server setting.

The want server flag, an internal setting, is used when the same server must be used for all stages of a multistage transaction regardless of the server cost. If the want server is not available, the transaction fails.

You can use the **load-balance method least-outstanding ignore-preferred-server** command if you have either of the following configurations:

- Dedicated authentication server and a separate dedicated accounting server
- Network where you can track all call record statistics and call record details, including start and stop records and records that are stored on separate servers

If you have a configuration where authentication servers are a superset of accounting servers, the preferred server is not used.

Note If a third-party RADIUS load balancer is used and RADIUS packets are routed based on the NAS source port, it is recommended to move to any other rule based on the following Attribute-Value Pairs (AVPs):

- If the load balancer uses NAS source port in the Access-Request to load balance, rules may not work as expected as the source port in NAS might change during transaction.
- If the load balancer compares AVPs between Access-Challenge and Access-Request to route packets, you will need to use the AVP value of t-State.
- If the load balancer compares AVPs in Access-Request from NAS, you will need to use one or a combination of the following AVPs:
  - t-State value
  - Calling-Station-ID and NAS IP or Identifier

Prerequisites for RADIUS Server Load Balancing

- Authentication, Authorization, and Accounting (AAA) must be configured on the RADIUS server.
- AAA RADIUS server groups must be configured.
- RADIUS must be configured for functions such as authentication, accounting, or static route download.

Restrictions for RADIUS Server Load Balancing

- Incoming RADIUS requests, such as Packet of Disconnect (POD) requests are not supported.
- Load balancing is not supported on proxy RADIUS servers and private server groups.
- Load balancing is not supported on Central Web Authentication (CWA).

Enabling Load Balancing for a Named RADIUS Server Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**aaa group server radius** *group-name* **Example:** `Device(config)# aaa group server radius rad-sg`	Enters server group configuration mode.
Step 3	**server ip-address** [**auth-port port-number**] [**acct-port port-number**] **Example:** `Device(config-sg-radius)# server 192.0.2.238 auth-port 2095 acct-port 2096`	Configures the IP address of the RADIUS server for the group server.
Step 4	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] **Example:** `Device(config-sg-radius)# load-balance method least-outstanding batch-size 30`	Enables the least-outstanding load balancing for a named server group. **Note** The session ownership change occurs multiple times when RADIUS server load balancing feature is configured with 802.1x authentication in Cisco ISE. This is because the RADIUS server load balancing feature distributes transactions of the same session in different RADIUS servers. Therefore, when the **Endpoint Owner Directory** is enabled in Cisco ISE, the RADIUS server load balancing feature is enabled in the controller and there is a high rate of 802.1x authentication or accounting requests resulting in the following: • High Authentication Latency for sessions in ISE. • Full RMQ queue (with size of 50000 endpoint profiler forwarder events). • Drop new endpoints sessions.
Step 5	**end** **Example:** `Device(config-sg)# end`	Exits server group configuration mode and enters privileged EXEC mode.

CHAPTER 104

AAA Dead-Server Detection

- Information About AAA Dead-Server Detection, on page 1167
- Prerequisites for AAA Dead-Server Detection, on page 1168
- Restrictions for AAA Dead-Server Detection, on page 1168
- Configuring AAA Dead-Server Detection (CLI), on page 1168
- Verifying AAA Dead-Server Detection, on page 1169

Information About AAA Dead-Server Detection

The AAA Dead-Server Detection feature allows you to configure the criteria to be used to mark a RADIUS server as dead.

If you have more than one RADIUS server, the following concepts come into picture:

- Deadtime—Defines the time in minutes a server marked as DEAD is held in that state. Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval.

Note You can configure deadtime for each server group or on a global level.

- Dead-criteria—To declare a server as DEAD, you need to configure **dead-criteria** and configure the conditions that determine when a RADIUS server is considered unavailable or dead.

Using this feature will result in less deadtime and quicker packet processing.

Criteria for Marking a RADIUS Server As Dead

The AAA Dead-Server Detection feature allows you to determine the criteria that are used to mark a RADIUS server as dead. That is, you can configure the minimum amount of time, in seconds, that must elapse from the time that the controller last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the controller booted, and there is a timeout, the time criterion will be treated as though it has been met.

In addition, you can configure the number of consecutive timeouts that must occur on the controller before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types

of packets are included in the number. Improperly constructed packets are counted as though they are timeouts. Both initial packet transmission and retransmissions are counted. (Each timeout causes one retransmission to be sent.)

Note Both the time criterion and tries criterion must be met for the server to be marked as dead.

The RADIUS dead-server detection configuration will result in the prompt detection of RADIUS servers that have stopped responding. This configuration will also result in the avoidance of servers being improperly marked as dead when they are "swamped" (responding slowly) and the avoidance of the state of servers being rapidly changed from dead to live to dead again. This prompt detection of non-responding RADIUS servers and the avoidance of swamped and dead-to-live-to-dead-again servers will result in less deadtime and quicker packet processing.

Prerequisites for AAA Dead-Server Detection

- You must have access to a RADIUS server.
- You should be familiar with configuring a RADIUS server.
- You should be familiar with configuring Authentication, Authorization, and Accounting (AAA).
- Before a server can be marked as dead, you must configure **radius-server dead-criteria time** *time-in-seconds* **tries** *number-of-tries* to mark the server as DOWN.

  Also, you must configure the **radius-server deadtime** *time-in-mins* to retain the server in DEAD status.

Restrictions for AAA Dead-Server Detection

- Original transmissions are not counted in the number of consecutive timeouts that must occur on the controller before the server is marked as dead--only the number of retransmissions are counted.

Configuring AAA Dead-Server Detection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA access control model.

	Command or Action	Purpose
Step 3	**radius-server deadtime** *time-in-mins* **Example:** `Device(config)# radius-server deadtime 5`	Defines the time in minutes when a server marked as DEAD is held in that state. Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval. *time-in-mins*—Valid values range from 1 to 1440 minutes. Default value is zero. To return to the default value, use the **no radius-server deadtime** command. The **radius-server deadtime** command can be configured globally or per aaa group server level. You can use the **show aaa dead-criteria** or **show aaa servers** command to check for dead-server detection. If the default value is zero, deadtime is not configured.
Step 4	**radius-server dead-criteria** [**time** *time-in-seconds*][**tries** *number-of-tries*] **Example:** `Device(config)# radius-server dead-criteria time 5 tries 4`	Declares a server as DEAD and configures the conditions that determine when a RADIUS server is considered unavailable or dead. *time-in-seconds*—Time in seconds during which no response is received from the RADIUS server to consider it as dead. Valid values range from 1 to 120 seconds. *number-of-tries*—Number of transmits to RADIUS server without responses before marking the server as dead. Valid values range from 1 to 100.
Step 5	**end** **Example:** `Device(config)# end`	Exits configuration mode and enters privileged EXEC mode.

Verifying AAA Dead-Server Detection

To verify dead-criteria, use the following command:

```
Device# show run | s dead-criteria

radius-server dead-criteria time 20 tries 20
```

To verify the dead-criteria details, use the following command:

```
Device# sh aaa dead-criteria radius <server>

sh aaa dead-criteria radius 8.109.0.55
RADIUS Server Dead Criteria:
Server Details:
Address : 8.109.0.55
Auth Port : 1645
Acct Port : 1646
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 5
Estimated Outstanding Access Transactions: 2
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 30s
Computed Retransmit Tries: 6
Statistics Gathered Since Last Successful Transaction
Max Computed Outstanding Transactions: 3
Max Computed Dead Detect Time: 90s
Max Computed Retransmits : 18
```

To verify the state of servers, number of requests being processed, and so on, use the following command:

```
Device# show aaa servers | s WNCD

Platform State from WNCD (1) : current UP
Platform State from WNCD (2) : current UP
Platform State from WNCD (3) : current UP
Platform State from WNCD (4) : current UP
Platform State from WNCD (5) : current UP, duration 773s, previous duration 0s
Platform Dead: total time 0s, count 0
Quarantined: No
```

CHAPTER 105

ISE Simplification and Enhancements

- Utilities for Configuring Security, on page 1171
- Configuring Captive Portal Bypassing for Local and Central Web Authentication, on page 1173
- Sending DHCP Options 55 and 77 to ISE, on page 1176
- Captive Portal, on page 1179

Utilities for Configuring Security

This chapter describes how to configure all the RADIUS server side configuration using the following command:

wireless-default radius server *ip* **key** *secret*

This simplified configuration option provides the following:

- Configures AAA authorization for network services, authentication for web auth and Dot1x.
- Enables local authentication with default authorization.
- Configures the default redirect ACL for CWA.
- Creates global parameter map with virtual IP and enables captive bypass portal.
- Configures all the AAA configuration for a default case while configuring the RADIUS server.
- The method-list configuration is assumed by default on the WLAN.
- Enables the radius accounting by default.
- Disables the radius aggressive failovers by default.
- Sets the radius request timeouts to 5 seconds by default.
- Enables captive bypass portal.

This command configures the following in the background:

```
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
!
aaa server radius dynamic-author
```

```
 client <IP> server-key cisco123
!
radius server RAD_SRV_DEF_<IP>
 description Configured by wireless-default
 address ipv4 <IP> auth-port 1812 acct-port 1813
 key <key>
!
aaa local authentication default authorization default
aaa session-id common
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host <IP>
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

Thus, you need not go through the entire Configuration Guide to configure wireless controller for a simple configuration requirement.

Configuring Multiple Radius Servers

Use the following procedure to configure a RADIUS server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless-default radius server** *ip* **key** *secret* **Example:** `Device(config)# wireless-default radius server 9.2.58.90 key cisco123`	Configures a radius server. **Note** You can configure up to ten RADIUS servers.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying AAA and Radius Server Configurations

To view details of AAA server, use the following command:

```
Device# show run aaa
!
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting Identity default start-stop group radius
!
aaa server radius dynamic-author
 client 9.2.58.90 server-key cisco123
!
radius server RAD_SRV_DEF_9.2.58.90
 description Configured by wireless-default
 address ipv4 9.2.58.90 auth-port 1812 acct-port 1813
 key cisco123
!
aaa local authentication default authorization default
aaa session-id common
!
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host 9.2.58.90
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

Note The **show run aaa** output may change when new commands are added to this utility.

Configuring Captive Portal Bypassing for Local and Central Web Authentication

Information About Captive Bypassing

WISPr is a draft protocol that enables users to roam between different wireless service providers. Some devices (For example, Apple iOS devices) have a mechanism using which they can determine if the device is connected

to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used for the device to automatically open a web browser when a direct connection to the internet is not possible. This enables the user to provide his credentials to access the internet. The actual authentication is done in the background every time the device connects to a new SSID.

The client device (Apple iOS device) sends a WISPr request to the controller , which checks for the user agent details and then triggers an HTTP request with a web authentication interception in the controller . After verification of the iOS version and the browser details provided by the user agent, the controller allows the client to bypass the captive portal settings and provides access to the Internet.

This HTTP request triggers a web authentication interception in the controller as any other page requests are performed by a wireless client. This interception leads to a web authentication process, which will be completed normally. If the web authentication is being used with any of the controller splash page features (URL provided by a configured RADIUS server), the splash page may never be displayed because the WISPr requests are made at very short intervals, and as soon as one of the queries is able to reach the designated server, any web redirection or splash page display process that is performed in the background is cancelled, and the device processes the page request, thus breaking the splash page functionality.

For example, Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to http://www.apple.com/library/test/success.html for Apple iOS version 6 and older, and to several possible target URLs for Apple iOS version 7 and later. If a response is received, then the Internet access is assumed to be available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an ISE captive portal. The controller prevents this pseudo-browser from popping up.

You can now configure the controller to bypass WISPr detection process, so the web authentication interception is only done when a user requests a web page leading to splash page load in user context, without the WISPr detection being performed in the background.

Configuring Captive Bypassing for WLAN in LWA and CWA (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 In the **Webauth Parameter Map** tab, click the parameter map name. The **Edit WebAuth Parameter** window is displayed.

Step 3 Select **Captive Bypass Portal** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Captive Bypassing for WLAN in LWA and CWA (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth WLAN1_MAP`	Creates the parameter map. The *parameter-map-name* must not exceed 99 characters.
Step 3	**captive-bypass-portal** **Example:** `Device(config)# captive-bypass-portal`	Configures captive bypassing.
Step 4	**wlan** *profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME`	Specifies the WLAN name and ID. • *profile-name* is the WLAN name which can contain 32 alphanumeric characters. • *wlan-id* is the wireless LAN identifier. The valid range is from 1 to 512. • *ssid-name* is the SSID which can contain 32 alphanumeric characters.
Step 5	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables the web authentication for the WLAN.
Step 6	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Maps the parameter map. **Note** If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Sending DHCP Options 55 and 77 to ISE

Information about DHCP Option 55 and 77

The DHCP sensors use the following DHCP options on the ISE for native and remote profiling:

- **Option 12**: Hostname
- **Option 6**: Class Identifier

Along with this, the following options needs to be sent to the ISE for profiling:

- **Option 55**: Parameter Request List
- **Option 77**: User Class

Configuration to Send DHCP Options 55 and 77 to ISE (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the**Policy Profile** page, click **Add** to view the **Add Policy Profile** window.

Step 3 Click **Access Policies** tab, choose the **RADIUS Profiling** and **DHCP TLV Caching** check boxes to configure radius profiling and DHCP TLV Caching on a WLAN.

Step 4 Click **Save & Apply to Device**.

Configuration to Send DHCP Options 55 and 77 to ISE (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**dhcp-tlv-caching** **Example:**	Configures DHCP TLV caching on a WLAN.

	Command or Action	Purpose
	`Device(config-wireless-policy)# dhcp-tlv-caching`	
Step 4	**radius-profiling** **Example:** `Device(config-wireless-policy)# radius-profiling`	Configures client radius profiling on a WLAN.
Step 5	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring EAP Request Timeout (GUI)

Follow the steps given below to configure the EAP Request Timeout through the GUI:

Procedure

Step 1 Choose **Configuration** > **Security** > **Advanced EAP**.

Step 2 In the **EAP-Identity-Request Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP identity request to wireless clients using local EAP.

Step 3 In the **EAP-Identity-Request Max Retries** field, specify the maximum number of times that the device attempts to retransmit the EAP identity request to wireless clients using local EAP.

Step 4 Set **EAP Max-Login Ignore Identity Response** to **Enabled** state to limit the number of clients that can be connected to the device with the same username. You can log in up to eight times from different clients (PDA, laptop, IP phone, and so on) on the same device. The default state is **Disabled**.

Step 5 In the **EAP-Request Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP request to wireless clients using local EAP.

Step 6 In the **EAP-Request Max Retries** field, specify the maximum number of times that the device attempts to retransmit the EAP request to wireless clients using local EAP.

Step 7 In the **EAPOL-Key Timeout** field, specify the amount of time (in seconds) in which the device attempts to send an EAP key over the LAN to wireless clients using local EAP.

Step 8 In the **EAPOL-Key Max Retries** field, specify the maximum number of times that the device attempts to send an EAP key over the LAN to wireless clients using local EAP.

Step 9 In the **EAP-Broadcast Key Interval** field, specify the time interval between rotations of the broadcast encryption key used for clients and click **Apply**.

Note After configuring the EAP-Broadcast key interval to a new time period, you must shut down or restart the WLAN for the changes to take effect. Once the WLAN is shut down or restarted, the M5 and M6 packets are exchanged when the configured timer value expires.

Configuring EAP Request Timeout

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps client-exclusion dot1x-timeout** **Example:** `Device(config)# wireless wps client-exclusion dot1x-timeout`	Enables exclusion on timeout and no response. By default, this feature is enabled. To disable, append a **no** at the beginning of the command.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring EAP Request Timeout in Wireless Security (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless security dot1x request** {**retries** *0 - 20* | **timeout** *1 - 120*} **Example:** `Device(config)# wireless security dot1x request timeout 60`	Configures the EAP request retransmission timeout value in seconds.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Captive Portal

Captive Portal Configuration

This feature enables you to configure multiple web authentication URLs (including external captive URLs) for the same SSID based on an AP. The default setting is to use the Global URL for authentication. The override option is available at WLAN and AP level.

The order of precedence is:

- AP
- WLAN
- Global configuration

Restrictions for Captive Portal Configuration

- This configuration is supported in a standalone controller only.
- Export-Anchor configuration is not supported.

Configuring Captive Portal (GUI)

Procedure

Step 1	Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2	Click **Add**.
Step 3	In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.
Step 4	In the **Security** > **Layer2** tab, uncheck the **WPA Policy**, **AES** and **802.1x** check boxes.
Step 5	In the **Security** > **Layer3** tab, choose the parameter map from the **Web Auth Parameter Map** drop-down list and authentication list from the **Authentication List** drop-down list.
Step 6	In the **Security** >**AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.
Step 7	Click **Apply to Device**.
Step 8	Choose **Configuration** > **Security** > **Web Auth**.
Step 9	Choose a **Web Auth Parameter Map**.
Step 10	In the **General** tab, enter the **Maximum HTTP connections**, **Init-State Timeout(secs)** and choose **webauth** from the **Type** drop-down list.
Step 11	In the **Advanced** tab, under the **Redirect to external server** settings, enter the **Redirect for log-in** server.
Step 12	Click **Update & Apply**.

Configuring Captive Portal

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** {*profile-name* | **shutdown**} *network-name* **Example:** `Device(config)# wlan edc6 6 edc`	Configures the WLAN profile. Enables or Disables all WLANs and creates the WLAN identifier. The profile-name and the SSID network name should be up to 32 alphanumeric charcters.
Step 3	**ip** {**access-group** | **verify**} **web** *IPv4-ACL-Name* **Example:** `Device(config-wlan)# ip access-group web CPWebauth`	Configures the WLAN web ACL. **Note** WLAN needs to be disabled before performing this operation.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.

Step 7	**security web-auth** {**authentication-list** *authentication-list-name* | **authorization-list** *authorization-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*}
	Example:
	`Device(config-wlan)# security web-auth authentication-list cp-webauth`
	`Device(config-wlan)# security web-auth parameter-map parMap6`
		Enables web authentication for WLAN. Here,
		• **authentication-list**
		authentication-list-name: Sets the authentication list for IEEE 802.1x.
		• **authorization-list**
		authorization-list-name: Sets the override-authorization list for IEEE 802.1x.
		• **on-macfilter-failure**: Enables Web authentication on MAC filter failure.

	Command or Action	Purpose
		• **parameter-map** *parameter-map-name*: Configures the parameter map. **Note** When **security web-auth** is enabled, you get to map the default **authentication-list** and global **parameter-map**. This is applicable for authentication-list and parameter-map that are not explicitly mentioned.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**exit** **Example:** `Device(config-wlan)# exit`	Exits from the WLAN configuration.
Step 10	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth parMap6`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 11	**parameter-map type webauth** *parameter-map-name* **Example:** `Device(config)# parameter-map type webauth parMap6`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 12	**type webauth** **Example:** `Device(config-params-parameter-map)# type webauth`	Configures the webauth type parameter.
Step 13	**timeout init-state sec** <*timeout-seconds*> **Example:** `Device(config-params-parameter-map)# timeout inti-state sec 3600`	Configures the WEBAUTH timeout in seconds. Valid range for the time in sec parameter is 60 seconds to 3932100 seconds.
Step 14	**redirect for-login** <*URL-String*> **Example:** `Device(config-params-parameter-map)# redirect for-login https://172.16.100.157/portal/login.html`	Configures the URL string for redirect during login.

	Command or Action	Purpose
Step 15	**exit** **Example:** `Device(config-params-parameter-map)# exit`	Exits the parameters configuration.
Step 16	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy policy_tag_edc6`	Configures policy tag and enters policy tag configuration mode.
Step 17	**wlan** *wlan-profile-name* **policy** *policy-profile-name* **Example:** `Device(config-policy-tag)# wlan edc6 policy policy_profile_flex`	Attaches a policy profile to a WLAN profile.
Step 18	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

Captive Portal Configuration - Example

The following example shows how you can have APs at different locations, broadcasting the same SSID but redirecting clients to different redirect portals:

Configuring multiple parameter maps pointing to different redirect portal:

```
parameter-map type webauth parMap1
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.3:8080/portal/PortalSetup.action?portal=cfdbce00-2ce2-11e8-b83c-005056a06b27
redirect portal ipv4 172.16.12.3
!
!
parameter-map type webauth parMap11
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.4:8443/portal/PortalSetup.action?portal=094e7270-3808-11e8-9797-02421e4cae0c
redirect portal ipv4 172.16.12.4
!
```

Associating these parameter maps to different WLANs:

```
wlan edc1 1 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap11
```

```
no shutdown
wlan edc2 2 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap1
no shutdown
```

Note All WLANs have identical SSIDs.

Associating WLANs to different policy tags:

```
wireless tag policy policy_tag_edc1
wlan edc1 policy policy_profile_flex
wireless tag policy policy_tag_edc2
wlan edc2 policy policy_profile_flex
```

Assigning these policy tags to the desired APs:

```
ap E4AA.5D13.14DC
policy-tag policy_tag_edc1
site-tag site_tag_flex
ap E4AA.5D2C.3CAC
policy-tag policy_tag_edc2
site-tag site_tag_flex
```

CHAPTER 106

RADIUS DTLS

- Information About RADIUS DTLS, on page 1185
- Prerequisites, on page 1187
- Configuring RADIUS DTLS Server, on page 1187
- Configuring DTLS Dynamic Author, on page 1192
- Enabling DTLS for Client, on page 1193
- Verifying the RADIUS DTLS Server Configuration, on page 1195
- Clearing RADIUS DTLS Specific Statistics, on page 1195

Information About RADIUS DTLS

The Remote Authentication Dial-In User Service (RADIUS) is a client or server protocol that provides centralized security for users attempting to gain management access to a network. The RADIUS protocol is a widely deployed authentication and authorization protocol that delivers a complete Authentication, Authorization, and Accounting (AAA) solution.

RADIUS DTLS Port

The RADIUS port (DTLS server) is used for authentication and accounting. The default DTLS server port is 2083.

You can change the RADIUS DTLS port number using **dtls port** *port_number*. For more information, see the Configuring RADIUS DTLS Port Number section.

Shared Secret

You can use **radius/dtls** as the shared secret, if you have enabled DTLS for a specific server.

Handling PAC for CTS Communication

You can download PAC from ISE for CTS communication. Once the PAC is downloaded, you need to encrypt all the CTS attributes with the PAC key instead of the shared secret.

The ISE then decrypts these attributes using PAC.

Session Management

The RADIUS client purely depends on the response from the DTLS server. If the session is ideal for ideal timeout, then the session must be closed.

In case of invalid responses, the sessions must be deleted.

If you need to send the radius packets over DTLS, the DTLS session needs to be re-established with the specific server.

Load Balancing

Multiple DTLS servers and load balancing methods are configured.

You need to select the AAA server to which the request needs to be sent. Then use the DTLS context of the specific server to encrypt the RADIUS packet and send it back.

Connection Timeout

After the encrypted RADIUS packet is sent, you need to start the retransmission timer. If you do not get a response before the retransmission timer expires, the packet is re-encrypted and re-transmitted.

You can continue for number of times as per the **dtls retries** configuration or till the default value. Once the number of tries exceeds the limit, the server becomes unavailable and responses are sent back to the AAA clients.

Note The default connection timeout is 5 seconds.

Connection Retries

As the RADIUS DTLS is UDP based, you need to retry the connection after a specific timeout interval for a specific number of retries.

After all retries are exhausted, the DTLS connection performs the following:

- Is marked as unsuccessful.
- Looks up for the next available server for processing the RADIUS requests.

Note The default connection retries is 5.

Idle Timeout

When the idle timer expires and no transactions exists since the last idle timeout, the DTLS session remains closed.

After you establish the DTLS session, you can start the idle timer. If you start the idle timer for 30 seconds and one of the RADIUS DTLS packet is sent, then after 30 seconds, the idle timer expires and checks for number of RADIUS DTLS transactions.

If the idle timer value exceeds zero, the idle timer resets the transaction counter and restarts the timer.

Note The default idle timeout is 60 seconds.

Handling Server and Server Group Failover

You can configure RADIUS servers with and without DTLS. It is recommended to create AAA server groups with DTLS enabled servers and non-DTLS servers. However, you will not find any such restriction while configuring AAA server groups.

Suppose you choose a DTLS server, the DTLS server establishes connection and RADIUS request packet is sent to the DTLS server. If the DTLS server does not respond after all RADIUS retries, it would fall over to the next configured server in the same server group. If the next server is a DTLS server, the processing of the RADIUS request packet continues with the next server. If the next server is a non-DTLS server, the processing of RADIUS request packet does not happen in that server group. Then the server group failover occurs and the same sequence continues with the next server group, if the next server group is available.

Note You need to use either only DTLS or non-DTLS servers in a server group.

Prerequisites

Support for IOS and BINOS AAA

The AAA server runs in IOS and BINOS platforms. Once you complete the RADIUS DTLS support in IOS, the same needs to be ported to BINOS.

Configuring RADIUS DTLS Server

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.

	Command or Action	Purpose
Step 4	**dtls** **Example:** `Device(config-radius-server)# dtls`	Configures DTLS parameters.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Connection Timeout

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls connectiontimeout** *timeout* **Example:** `Device(config-radius-server)# dtls connectiontimeout 1`	Configures RADIUS DTLS connection timeout. Here, *timeout* refers to the DTLS connection timeout value. The valid range is from 1 to 65535.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Idle Timeout

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enters privileged EXEC mode.

	Command or Action	Purpose
	`Device# enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls idletimeout** *idle_timeout* **Example:** `Device(config-radius-server)# dtls idletimeout 2`	Configures RADIUS DTLS idle timeout. Here, *idle_timeout* refers to the DTLS idle timeout value. The valid range is from 1 to 65535.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Source Interface for RADIUS DTLS Server

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls ip** {**radius source-interface Ethernet-Internal** *interface_number* **Example:** `Device(config-radius-server)# dtls ip radius source-interface Ethernet-Internal 0`	Configures source interface for RADIUS DTLS server. Here, • *interface_number* refers to the Ethernet-Internal interface number. The default value is 0.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Port Number

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls port** *port_number* **Example:** `Device(config-radius-server)# dtls port 2`	Configures RADIUS DTLS port number. Here, *port_number* refers to the DTLS port number.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Connection Retries

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.
Step 4	**dtls retries** *retry_number* **Example:** `Device(config-radius-server)# dtls retries 3`	Configures RADIUS connection retries. Here, *retry_number* refers to the DTLS connection retries. The valid range is from 1 to 65535.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Trustpoint

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server R1`	Specifies the RADIUS server name.

Step 4	**dtls trustpoint** {**client** *LINE* **dtls** | **server** *LINE* **dtls**}
	Example:
	`Device(config-radius-server)# dtls trustpoint client client1 dtls`
	`Device(config-radius-server)# dtls trustpoint server server1 dtls`
		Configures trustpoint for client and server.

Step 5	**end** **Example:** `Device(config-radius-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring RADIUS DTLS Match-Server-Identity

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `dtls match-server-identity hostname <name>`	Configure the RADSEC certification validation parameters.
Step 2	**enable** **Example:** `dtls match-server-identity ip-address <IPv4 or IPv6>`	Configure the RADSEC certification validation parameters.

Configuring DTLS Dynamic Author

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures local server profile for RFC 3576 support.
Step 4	**dtls** **Example:** `Device(config-locsvr-da-radius)# dtls`	Configures DTLS source parameters.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling DTLS for Client

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures local server profile for RFC 3576 support.
Step 4	**client** *IP_addr* **dtls** **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls`	Enables DTLS for the client.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Client Trustpoint for DTLS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:**	Configures local server profile for RFC 3576 support.

	Command or Action	Purpose
	`Device(config)# aaa server radius dynamic-author`	
Step 4	**client** *IP_addr* **dtls** {**client-tp** *client-tp-name* | **server-tp** *server-tp-name*} **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls client-tp client_tp_name`	Configures client trustpoint for DTLS.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring DTLS Idle Timeout

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures local server profile for RFC 3576 support.
Step 4	**client** *IP_addr* **dtls idletimeout** *timeout-interval* {**client-tp** *client_tp_name* | **server-tp** *server_tp_name*} **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 62 client-tp dtls_ise`	Configures DTLS idle time. Here, *timeout-interval* refers to the idle timeout interval. The valid range is from 60 to 600.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Server Trustpoint for DTLS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures local server profile for RFC 3576 support.
Step 4	**client** *IP_addr* **dtls server-tp** *server_tp_name* **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls server-tp dtls_client`	Configures server trust point.
Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying the RADIUS DTLS Server Configuration

To view information about the DTLS enabled servers, use the following command:

```
Device# show aaa servers
DTLS: Packet count since last idletimeout 1,
Send handshake count 3,
Handshake Success 1,
Total Packets Transmitted 1,
Total Packets Received 1,
Total Connection Resets 2,
Connection Reset due to idle timeout 0,
Connection Reset due to No Response 2,
Connection Reset due to Malformed packet 0,
```

Clearing RADIUS DTLS Specific Statistics

To clear the radius DTLS specific statistics, use the following command:

```
Device# clear aaa counters servers radius {<server-id> | all}
```

Note Here, *server-id* refers to the server ID displayed by **show aaa servers**. The valid range is from 0 to 2147483647.

CHAPTER 107

Policy Enforcement and Usage Monitoring

- Policy Enforcement and Usage Monitoring, on page 1197
- Configuring Policy Enforcement and Enabling Change-of-Authorization (CLI), on page 1197
- Example: Configuring Policy Enforcement and Usage Monitoring, on page 1198
- Verifying Policy Usage and Enforcement, on page 1199

Policy Enforcement and Usage Monitoring

You can enforce dynamic QoS policies and upstream and downstream TCP or UDP data rates on 802.11 clients seamlessly without disrupting the client's ongoing sessions. The feature ensures that clients do not have to get dissociated from the network. All the authentication methods: 802.1X, PSK, web authentication, and so on, are supported.

The APs periodically send client statistics including bandwidth usage to the Controller. The AAA server receives Accounting-Interim messages which include the clients data utilization at the configured intervals. The AAA server accumulates information about data consumption for each client and when the client exhausts the data limit, the AAA server sends a change-of-authorization (CoA) message to the Controllers. Upon successful CoA handshakes, the Controllers apply and send new policies to the APs.

Restrictions on Policy Enforcement and Usage Monitoring

- Only FlexConnect local switching mode is supported.

Configuring Policy Enforcement and Enabling Change-of-Authorization (CLI)

For more information, follow the utility specified in Utilities for configuring Security section of this guide.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Creates a local server RADIUS profile in the controller.
Step 3	**client** *client-ip-addr* **server-key** *key* **Example:** `Device(config-locsvr-da-radius)# client 3.2.4.3 server-key testpwd`	Configures a server key for a RADIUS client.
Step 4	**[Optional] show aaa command handler** **Example:** `Device#show aaa command handler`	Displays the AAA CoA packet statistics.

Example: Configuring Policy Enforcement and Usage Monitoring

Policy enforcement and usage monitoring is applied on a group where a class-map is created for QOS policies. This is done via CoA.

Given below is a sample configuration for policy enforcement and usage monitoring:

```
aaa new-model
  radius server radius_free
  address ipv4 10.0.0.1 auth-port 1812 acct-port 1813
  key cisco123
  exit

aaa new-model
  aaa server radius dynamic-author
  client 10.0.0.1 server-key cisco123
aaa new-model
  aaa group server radius rad_eap
  server name radius_free
  exit
aaa new-model
  dot1x system-auth-control
  aaa authentication dot1x eap_methods group rad_eap
  dot1x system-auth-control
class-map client_dscp_clsmapout
match dscp af13
exit
class-map client_dscp_clsmapin
match dscp af13
exit
policy-map qos_new
  class client_dscp_clsmapout
  police 512000 conform-action transmit exceed-action drop
  policy-map qos_nbn
  class client_dscp_clsmapin
  police 16000000 conform-action transmit exceed-action drop
wlan test1 3 test2
```

```
  broadcast-ssid
  security wpa wpa2 ciphers aes
  security dot1x authentication-list eap_methods
no shutdown
exit
wireless profile policy named-policy-profile
shutdown
  vlan 10
  aaa-override
  no central association
  no central dhcp
  no central switching
  no shutdown
wireless tag policy named-policy-tag
  wlan test1 policy named-policy-profile
wireless profile flex FP_name_001
  native-vlan-id 10
wireless tag site ST_name_001
  no local-site
  flex-profile FP_name_001
  exit
ap test-ap
  policy-tag named-policy-tag
  site-tag ST_name_001
  exit
aaa authorization network default group radius
exit
```

Verifying Policy Usage and Enforcement

To view the detailed information about the policies applied to a specific client, use the following command:

```
Device# show wireless client mac-address mac-address detail
```

To view client-level mobility statistics, use the following command:

```
Device# show wireless client mac-address mac-address mobility statistics
```

To view client-level roaming history for an active client in a sub-domain, use the following command:

```
Device# show wireless client mac-address mac-address mobility history
```

To view detailed parameters of a given profile policy, use the following command:

```
Device# show wireless profile policy detailed policy-name
```

CHAPTER 108

Local Extensible Authentication Protocol

- Information About Local EAP, on page 1201
- Restrictions for Local EAP, on page 1202
- Configuring Local EAP Profile (CLI), on page 1202
- Configuring Local EAP profile (GUI), on page 1203
- Configuring AAA Authentication (GUI), on page 1203
- Configuring AAA Authorization Method (GUI), on page 1203
- Configuring AAA Authorization Method (CLI), on page 1204
- Configuring Local Advanced Methods (GUI), on page 1205
- Configuring WLAN (GUI), on page 1205
- Configuring WLAN (CLI), on page 1206
- Creating a User Account (CLI), on page 1206
- Attaching a Policy Profile to a WLAN Interface (GUI), on page 1207
- Deploy Policy Tag to Access Points (GUI), on page 1208

Information About Local EAP

Local Extensible Authentication Protocol (EAP) feature refers to the controller that acts as authenticator and authentication server. Local EAP allows 802.1x authentication on WPA Enterprise wireless clients without the use of any RADIUS server. The Local EAP refers to the EAP authentication server activity and not necessarily tied to the user credentials validation (for example) that can be delegated to an external LDAP database.

Feature Scenarios

Local EAP is designed to allow administrators to use Enterprise-grade 802.1x authentication for a limited number of users in situations and branches where an external dedicated RADIUS server may not be available. It can also work as an emergency backup in case the RADIUS server is not available.

Use Cases

You can implement Local EAP either with users local to the controller or use an external LDAP database to store the user credentials.

Restrictions for Local EAP

- It is not possible to configure AAA attributes, such as per-user ACL or per-user session timeout using local EAP.
- Local EAP only allows user database either locally on the controller or on an external LDAP database.
- Local EAP supports TLS 1.2 as of 17.1 and later software release.
- Local EAP uses the trustpoint of your choice on the controller. You will either need to install a publicly trusted certificate on the controller or import it on the clients for the EAP session to be trusted by the client.
- Local EAP supports *EAP-FAST*, *EAP-TLS*, and *PEAP* as EAP authentication methods.

Note *PEAP-mschapv2* does not work when using certain external LDAP databases that only support clear text passwords.

Configuring Local EAP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**eap profile** *name* **Example:** `Device(config)# eap profile mylocapeap`	Creates an EAP profile.
Step 3	**method peap** **Example:** `Device(config-eap-profile)# method peap`	Configures the PEAP method on the profile.
Step 4	**pki-trustpoint** *name* **Example:** `Device(config-eap-profile)# pki-trustpoint admincert`	Configures the PKI trustpoint on the profile.

Configuring Local EAP profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local EAP**.

Step 2 Click **Add**.

Step 3 In the **Create Local EAP Profiles** page, enter a profile name.

Note It is not advised to use LEAP EAP method due to its weak security. You can use any of the following EAP methods to configure a trustpoint:

- EAP-FAST
- EAP-TLS
- PEAP

Clients do not trust the default controller certificate, so you need to deactivate the server certificate validation on the client side or install a certificate trustpoint on the controller.

Step 4 Click **Apply to Device**.

Configuring AAA Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**, and navigate to the **AAA Method List** > **Authentication** tabs.

Step 2 Click **Add**.

Step 3 Choose **dot1x** as the **Type** and **local** as the **Group Type**.

Step 4 Click **Apply to Device**.

Configuring AAA Authorization Method (GUI)

Procedure

Step 1 Navigate to **Authorization** sub-tab.

Step 2 Create a new method for **credential-download** type and point it to local.

Note Perform the same for **network** authorization type.

Configuring AAA Authorization Method (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 3	**aaa authentication dot1x default local** **Example:** `Device(config)# aaa authentication dot1x default local`	Configures the default local RADIUS server.
Step 4	**aaa authorization credential-download default local** **Example:** `Device(config)# aaa authorization credential-download default local`	Configures default database to download credentials from local server.
Step 5	**aaa local authentication default authorization default** **Example:** `Device(config)# aaa local authentication default authorization default`	Configures the local authentication method list.
Step 6	**aaa authorization network default local** **Example:** `Device(config)# aaa authorization network default local`	Configures authorization for network services.

Configuring Local Advanced Methods (GUI)

Procedure

Step 1 In the **Configuration** > **Security** > **AAA** window, perform the following:

a. Navigate to **AAA Advanced** tab.

b. From the **Local Authentication** drop-down list, choose a default local authentication.

c. From the **Local Authorization** drop-down list, choose a default local authorization.

Step 2 Click **Apply**.

Configuring WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 In the **WLANs** window, click the name of the **WLAN** or click **Add** to create a new one.

Step 3 In the **Add/Edit WLAN** window that is displayed, click the **General** tab to configure the following parameters.

- In the **Profile Name** field, enter or edit the name of the profile.
- In the **SSID** field, enter or edit the SSID name.

  The SSID name can be alphanumeric, and up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number. The valid range is between 1 and 512.
- From the **Radio Policy** drop-down list, choose the **802.11** radio band.
- Using the **Broadcast SSID** toggle button, change the status to either **Enabled** or **Disabled**.
- Using the **Status** toggle button, change the status to either **Enabled** or **Disabled**.

Step 4 In the **AAA** tab, you can configure the following:

a. Choose an authentication list from the drop-down.

b. Check the **Local EAP Authentication** check box to enable local EAP authentication on the WLAN. Also, choose the required **EAP Profile Name** from the drop-down list.

Step 5 Click **Save & Apply to Device**.

Configuring WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan localpeapssid 1 localpeapssid`	Enters the WLAN configuration sub-mode. *wlan-name*—Is the name of the configured WLAN. *wlan-id*—Is the wireless LAN identifier. The range is 1 to 512. *SSID-name*—Is the SSID name which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *wlan-name* command.
Step 3	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 4	**local-auth** *profile name* **Example:** `Device(config-wlan)# local-auth mylocaleap`	Sets EAP Profile on an WLAN. *profile name*—Is the EAP profile on an WLAN.

Creating a User Account (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**user-name** *user-name* **Example:** `Device(config)# user-name 1xuser`	Creates a user account.
Step 3	**creation-time** *time* **Example:** `Device(config)# creation-time 1572730075`	Creation time of the user account.
Step 4	**description** *user-name* **Example:** `Device(config)# description 1xuser`	Adds a user-defined description to the new user account.
Step 5	**password 0** *password* **Example:** `Device(config)# password 0 Cisco123`	Creates a password for the user account.
Step 6	**type network-user description** *user-name* **Example:** `Device(config)# type network-user description 1xuser`	Specifies the type of user account.

Attaching a Policy Profile to a WLAN Interface (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.
Step 2 On the **Manage Tags** page, click **Policy** tab.
Step 3 Click **Add** to view the **Add Policy Tag** window.
Step 4 Enter a name and description for the policy tag.
Step 5 Click **Add** to map the WLAN and policy.
Step 6 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.
Step 7 Click **Save & Apply to Device**.

Deploy Policy Tag to Access Points (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **All Access Points** page, click the access point you want to configure.

Make sure that the tags assigned are the ones you configured.

Step 3 Click **Apply**.

CHAPTER 109

Local EAP Ciphersuite

- Information About Local EAP Ciphersuite, on page 1209
- Restrictions for Local EAP Ciphersuite, on page 1210
- Configuring Local EAP Ciphersuite (CLI), on page 1211

Information About Local EAP Ciphersuite

Prior to Cisco IOS XE Cupertino 17.7.1 Release, the controller acts as an SSL server supporting a hardcoded list of ciphersuites for each EAP application. From Cisco IOS XE Cupertino 17.7.1 Release onwards, the controller is equipped with a knob that controls the list of ciphersuites when using local authentication.

The following table lists the hardcoded list of ciphersuites:

Table 79: Hardcoded List of Ciphersuites

Ciphersuites	Description
aes128-sha	Encryption Type tls_rsa_with_aes_128_cbc_sha.
aes256-sha	Encryption Type tls_rsa_with_aes_256_cbc_sha.
dhe-rsa-aes-gcm-sha2	Encryption Type tls_dhe_rsa_with_aes_128_gcm_sha256 and tls_dhe_rsa_with_aes_256_gcm_sha384(TLS1.2 and above).
dhe-rsa-aes-sha2	Encryption Type tls_dhe_rsa_with_aes_128_cbc_sha256 and tls_dhe_rsa_with_aes_256_cbc_sha256 (TLS 1.2 and above).
dhe-rsa-aes128-sha	Encryption Type tls_dhe_rsa_with_aes_128_cbc_sha.
dhe-rsa-aes256-sha	Encryption Type tls_dhe_rsa_with_aes_256_cbc_sha.
ecdhe-ecdsa-aes-gcm-sha2	Encryption Type tls_ecdhe_ecdsa_with_aes_128_gcm_sha256 and tls_ecdhe_ecdsa_with_aes_256_gcm_sha384(TLS1.2 and above).

Ciphersuites	Description
ecdhe-ecdsa-aes-sha	Encryption Type tls_ecdhe_ecdsa_with_aes_128_cbc_sha and tls_ecdhe_ecdsa_with_aes_256_cbc_sha.
ecdhe-ecdsa-aes-sha2	Encryption Type tls_ecdhe_ecdsa_with_aes_128_cbc_sha256 and tls_ecdhe_ecdsa_with_aes_256_cbc_sha384(TLS1.2 and above).
ecdhe-rsa-aes-gcm-sha2	Encryption Type tls_ecdhe_rsa_with_aes_128_gcm_sha256 and tls_ecdhe_rsa_with_aes_256_gcm_sha384(TLS1.2 and above).
ecdhe-rsa-aes-sha	Encryption Type tls_ecdhe_rsa_with_aes_128_cbc_sha and tls_ecdhe_rsa_with_aes_256_cbc_sha.
ecdhe-rsa-aes-sha2	Encryption Type tls_ecdhe_rsa_with_aes_128_cbc_sha256 and tls_ecdhe_rsa_with_aes_256_cbc_sha384(TLS1.2 and above).

When the Client and Server Hello messages are exchanged, the client sends a prioritized list of ciphersuites it supports in Client Hello. The server then responds with the ciphersuite selected from the list in Server Hello. The server needs to select a ciphersuite that is acceptable to both the client and server. Using this approach, only one ciphersuite is selected and sent to the client.

The Local EAP ciphersuite feature controls the list of ciphersuites the controller as SSL server supports.

Note By default, all the ciphersuites are supported. Using the Local EAP ciphersuite feature, you can enable or disable the ciphersuites based on your requirement.

Restrictions for Local EAP Ciphersuite

- SNMP is not supported.
- Ciphersuites are specific to Dot1x.

Configuring Local EAP Ciphersuite (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**eap profile** *name* **Example:** `Device(config)# eap profile local_EAP_TLSv1`	Creates an EAP profile.
Step 4	**ciphersuite** *cipher-suite* **Example:** `Device(config-eap-profile)# ciphersuite <cipher-suite>`	Select a ciphersuite. **Note** Using this command, you will be able to configure only one ciphersuite. To configure more than one ciphersuite, you need to issue this command with various ciphersuites. To remove the ciphersuites, you need to remove the ciphersuites one by one or all at once. By default all ciphersuites are supported, if you issue the **no ciphersuite** command.
Step 5	**end** **Example:** `Device(config-eap-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

CHAPTER 110

Authentication and Authorization Between Multiple RADIUS Servers

- Information About Authentication and Authorization Between Multiple RADIUS Servers, on page 1213
- Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers, on page 1214
- Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers, on page 1219
- Verifying Split Authentication and Authorization Configuration, on page 1221
- Configuration Examples, on page 1222

Information About Authentication and Authorization Between Multiple RADIUS Servers

Cisco Catalyst 9800 Series Wireless Controller uses the approach of request and response transaction with a single RADIUS server that combines both authentication and authorization. You can split the authentication and authorization on the controller between multiple RADIUS servers.

A RADIUS sever can assume the role of either an authentication server, authorization server, or both. In cases where there are disparate RADIUS servers for authentication and authorization, the Session Aware Networking (SANet) component on the controller now allows authentication on one server and authorization on another when a client joins the controller .

Authentication can be done using the Cisco ISE, Cisco Catalyst Center, Free RADIUS, or any third-party RADIUS Server. After successful authentication from an authentication server, the controller relays attributes received from the authentication server to another RADIUS sever designated as authorization server.

The authorization server then performs the following:

- Processes received attributes with the other policies or rules defined on the server.
- Derives attributes as part of the authorization response and returns it to the controller .

Note In a split authentication and authorization configuration, both servers must be available and must successfully authenticate and authorize with an ACCESS-ACCEPT for a session to be accepted by the controller .

Note A maximum of 100 entries is supported in the Authentication/Authorization list created through Cisco Catalyst Center provisioning. The entries beyond 100 do not work even though they can be created.

Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers

Configuring Explicit Authentication and Authorization Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**.

Step 2 On the **Authentication Authorization and Accounting** page, click the **Servers/Groups** tab.

Step 3 Click the type of AAA server you want to configure from the following options:

- RADIUS
- TACACS+
- LDAP

In this procedure, the RADIUS server configuration is described.

Step 4 With the **RADIUS** option selected, click **Add**.

Step 5 Enter a name for the RADIUS server and the IPv4 or IPV6 address of the server.

Step 6 Enter the authentication and encryption key to be used between the device and the key string RADIUS daemon running on the RADIUS server. You can choose to use either a PAC key or a non-PAC key.

Step 7 Enter the server timeout value; valid range is 1 to 1000 seconds.

Step 8 Enter a retry count; valid range is 0 to 100.

Step 9 Leave the **Support for CoA** field in **Enabled** state.

Step 10 Click **Save & Apply to Device**.

Step 11 On the **Authentication Authorization and Accounting** page, with **RADIUS** option selected, click the **Server Groups** tab.

Step 12 Click **Add**.

Step 13 In the **Create AAA RADIUS Server Group** window that is displayed, enter a name for the RADIUS server group.

Step 14 From the **MAC-Delimiter** drop-down list, choose the delimiter to be used in the MAC addresses that are sent to the RADIUS servers.

Step 15 From the **MAC Filtering** drop-down list, choose a value based on which to filter MAC addresses.

Step 16 To configure dead time for the server group and direct AAA traffic to alternative groups of servers that have different operational characteristics, in the **Dead-Time** field, enter the amount of time, in minutes, after which a server is assumed to be dead.

Step 17 Choose the servers that you want to include in the server group from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 18 Click **Save & Apply to Device**.

Configuring Explicit Authentication Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups**.

Step 2 Choose **RADIUS** > **Servers** tab.

Step 3 Click **Add** to add a new server or click an existing server.

Step 4 Enter the **Name**, the **Server Address**, **Key**, **Confirm Key**, **Auth Port** and **Acct Port.** Check the **PAC Key** checkbox and enter the **PAC key** and **Confirm PAC Key**

Step 5 Click **Apply to Device**.

Step 6 Choose **RADIUS** > **Server Groups** and click **Add** to add a new server group or click an existing server group.

Step 7 Enter the **Name** of the server group and choose the servers that you want to include in the server group, from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 8 Click **Apply to Device**.

Configuring Explicit Authentication Server List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server free-radius-authc-server`	Specifies the RADIUS server name.
Step 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* **Example:**	Specifies the RADIUS server parameters.

	Command or Action	Purpose
	`Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813`	
Step 5	[**pac**] **key** *key* **Example:** `Device(config-radius-server)# key cisco`	Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 7	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authc-server-group`	Creates a radius server-group identification. *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters. If the IP address of the RADIUS server is not added to the routes defined for the controller, the default route is used. We recommend that you define a specific route to source the traffic from the defined SVI in the AAA server group.
Step 8	**server name** *server-name* **Example:** `Device(config)# server name free-radius-authc-server`	Configures the server name.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. For more information, see **Configuring AAA for External Authentication**.

Configuring Explicit Authorization Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups**.

Step 2 Choose **RADIUS** > **Servers** tab.

Step 3 Click **Add** to add a new server or click an existing server.

Step 4 Enter the **Name**, the **Server Address**, **Key**, **Confirm Key**, **Auth Port** and **Acct Port.** Check the **PAC Key** checkbox and enter the **PAC key** and **Confirm PAC Key**

Step 5 Click **Apply to Device**.

Step 6 Choose **RADIUS** > **Server Groups** and click **Add** to add a new server group or click an existing server group.

Step 7 Enter the **Name** of the server group and choose the servers that you want to include in the server group, from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 8 Click **Apply to Device**.

Configuring Explicit Authorization Server List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server cisco-catalyst-center-authz-server`	Specifies the RADIUS server name.
Step 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* **Example:** `Device(config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813`	Specifies the RADIUS server parameters.
Step 5	[**pac**] **key** *key* **Example:** `Device(config-radius-server)# pac key cisco`	Specify the authorization and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 7	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authz-server-group`	Creates a radius server-group identification. **Note** *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.

	Command or Action	Purpose
Step 8	**server name** *server-name* **Example:** `Device(config)# server name cisco-catalyst-center-authz-server`	
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Authentication and Authorization List for 802.1X Security (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 In the **Security** > **AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.

Step 5 Click **Apply to Device**.

Configuring Authentication and Authorization List for 802.1X Security

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-foo 222 foo-ssid`	Enters WLAN configuration sub-mode. • *wlan-name*: Is the name of the configured WLAN. • *wlan-id*: Is the wireless LAN identifier. Range is from 1 to 512. • *SSID-name*: Is the SSID name which can contain 32 alphanumeric characters.

	Command or Action	Purpose
		Note If you have already configured this command, enter **wlan** *wlan-name* command.
Step 4	**security dot1x authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list authc-server-group`	Enables authentication list for dot1x security.
Step 5	**security dot1x authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security dot1x authorization-list authz-server-group`	Specifies authorization list for dot1x security. For more information on the **Cisco Catalyst Center**, see the **Cisco Catalyst Center documentation**.
Step 6	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers

Configuring Authentication and Authorization List for Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 In the **Security** > **Layer2** tab, uncheck the **WPAPolicy**, **AES** and **802.1x** check boxes.

Step 5 Check the **MAC Filtering** check box to enable the feature. With MAC Filtering enabled, choose the Authorization list from the **Authorization List** drop-down list.

Step 6 In the **Security** > **AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Configuring Authentication and Authorization List for Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-bar 1 bar-ssid`	Enters WLAN configuration sub-mode. • *wlan-name*: Is the name of the configured WLAN. • *wlan-id*: Is the wireless LAN identifier. • *SSID-name*: Is the SSID name which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *wlan-name* command.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**security web-auth** {**authentication-list** *authenticate-list-name* | **authorization-list** *authorize-list-name*}	Enables authentication or authorization list for dot1x security.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth authentication-list authc-server-group`	**Note** You get to view the following error, if you do not disable WPA security, AKM for dot1x, and WPA2 security: *% switch-1:dbm:wireless:web-auth cannot be enabled. Invalid WPA/WPA2 settings.*
Step 8	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Split Authentication and Authorization Configuration

To view the WLAN details, use the following command:

```
Device# show run wlan
wlan wlan-foo 2 foo-ssid
security dot1x authentication-list authc-server-group
security dot1x authorization-list authz-server-group

wlan wlan-bar 3 bar-ssid
security web-auth authentication-list authc-server-group
security web-auth authorization-list authz-server-group
```

To view the AAA authentication and server details, use the following command:

```
Device# show run aaa
!
aaa authentication dot1x default group radius
username cisco privilege 15 password 0 cisco
!
!
radius server free-radius-authc-server
 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
 key cisco
!
radius server cisco-catalyst-center-authz-server
 address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
 pac key cisco
!
!
aaa new-model
aaa session-id common
!
```

To view the authentication and authorization list for 802.1X security, use the following command:

```
Device# show wlan name wlan-foo | sec 802.1x
802.1x authentication list name               : authc-server-group
802.1x authorization list name                : authz-server-group
            802.1x                            : Enabled
```

To view the authentication and authorization list for web authentication, use the following command:

```
Device# show wlan name wlan-bar | sec Webauth
    Webauth On-mac-filter Failure             : Disabled
    Webauth Authentication List Name          : authc-server-group
    Webauth Authorization List Name           : authz-server-group
    Webauth Parameter Map                     : Disabled
```

Configuration Examples

Configuring Cisco Catalyst 9800 Series Wireless Controller for Authentication with a Third-Party RADIUS Server: Example

This example shows how to configure Cisco Catalyst 9800 Series Wireless Controller for authentication with a third-party RADIUS server:

```
Device(config)# radius server free-radius-authc-server
Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
Device(config-radius-server)# key cisco
Device(config-radius-server)# exit
Device(config)# aaa group server radius authc-server-group
Device(config)# server name free-radius-authc-server
Device(config)# end
```

Configuring Cisco Catalyst 9800 Series Wireless Controller for Authorization with Cisco ISE or Cisco Catalyst Center: Example

This example shows how to configure Cisco Catalyst 9800 Series Wireless Controller for authorization with Cisco ISE or Cisco Catalyst Center:

```
Device(config)# radius server cisco-catalyst-center-authz-server
Device (config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
Device (config-radius-server)# pac key cisco
Device (config-radius-server)# exit
Device(config)# aaa group server radius authz-server-group
Device(config)# server name cisco-catalyst-center-authz-server
Device(config)# end
```

CHAPTER 111

CUI Information in RADIUS Accounting

- CUI Information in RADIUS Accounting Request, on page 1223
- Adding CUI Information in a RADIUS Accounting Request, on page 1224
- Verifying CUI Information in a RADIUS Accounting Request, on page 1224

CUI Information in RADIUS Accounting Request

Chargeable User Identity (CUI) is a unique identifier for a client visiting a network regardless of the outer identity or the device used for login. In other words, CUI is an obscured version of a username. A client must be authenticated and authorized before being allowed to the network. The CUI attribute can be used as an alternative for a client's username as part of the authentication process.

To handle RADIUS attribute 89 processing, a null value of CUI is attached an access-request sent to a AAA server. This is done using the **access-session wireless cui-enable** command. As part of an access-accept message, a CUI-capable AAA server sends the CUI string to the controller. The controller then sends this received CUI attribute in accounting packets and other access-request packets, if any.

Prerequisites

Ensure that AAA override is enabled.

Restrictions

- Only 802.1x network authentication protocol is supported.
- Inter-Release Controller Mobility (IRCM) is not supported.
- FlexConnect local authentication is not supported. Only local mode and FlexConnect central authentication mode is supported.

Adding CUI Information in a RADIUS Accounting Request

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**access-session wireless cui-enable** **Example:** `Device(config)# access-session wireless cui-enable`	Adds CUI attribute in authentication and accounting messages sent to the AAA server.

Verifying CUI Information in a RADIUS Accounting Request

To view the CUI attribute in an accounting request on aAAA server, use the following command:

```
Device# show wireless client mac-address aaa.bbb.ccc.ddd detail
.
.
.
Session Manager:
  Point of Attachment : capwap_90000005
  IIF ID              : 0x90000005
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 8A45400A0000000CE0527C5F
  Acct Session ID  : 0x00000003
  Last Tried Aaa Server Details:
        Server IP : 10.64.69.141
  Auth Method Status List
        Method : Dot1x
                SM State         : AUTHENTICATED
                SM Bend State    : IDLE
  Local Policies:
        Service Template : wlan_svc_default-policy-profile_local (priority 254)
                VLAN             : 59
                Absolute-Timer   : 1800
  Server Policies:
                CUI              : 13e158006855c2ff718cc84487653f5a6ea55def
  Resultant Policies:
                CUI              : 13e158006855c2ff718cc84487653f5a6ea55def
                VLAN Name        : VLAN0059
                VLAN             : 59
                Absolute-Timer   : 1800
```

CHAPTER 112

Secure LDAP

- Information About SLDAP, on page 1225
- Prerequisite for Configuring SLDAP, on page 1227
- Restrictions for Configuring SLDAP, on page 1227
- Configuring SLDAP, on page 1227
- Configuring an AAA Server Group (GUI), on page 1228
- Configuring a AAA Server Group, on page 1229
- Configuring Search and Bind Operations for an Authentication Request, on page 1230
- Configuring a Dynamic Attribute Map on an SLDAP Server, on page 1231
- Verifying the SLDAP Configuration, on page 1231

Information About SLDAP

Transport Layer Security (TLS)

The Transport Layer Security (TLS) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. TLS relies upon certificates, public keys, and private keys to prove the identity of clients.

The certificates are issued by the Certificate Authorities (CAs).

Each certificate includes the following:

- The name of the authority that issued it.
- The name of the entity to which the certificate was issued.
- The public key of the entity.
- The timestamps of the entity that indicate the expiration date of the certificate.

You can find the TLS support for LDAP in the RFC2830 which is an extension to the LDAP protocol.

LDAP Operations

Bind

The bind operation is used to authenticate a user to the server. It is used to start a connection with the LDAP server. LDAP is a connection-oriented protocol. The client specifies the protocol version and authentication information.

LDAP supports the following binds:

- Authenticated bind—An authenticated bind is performed when a root Distinguished Name (DN) and password are available.
- Anonymous bind—In the absence of a root DN and password, an anonymous bind is performed.

In LDAP deployments, the search operation is performed first and the bind operation later. This is because, if a password attribute is returned as part of the search operation, the password verification can be done locally on an LDAP client. Thus, there is no need to perform an extra bind operation. If a password attribute is not returned, the bind operation can be performed later. Another advantage of performing a search operation first and a bind operation later is that the DN received in the search result can be used as the user DN instead of forming a DN by prefixing the username (cn attribute) with the base DN. All entries stored in an LDAP server have a unique DN.

The DN consists of two parts:

- Relative Distinguished Name (RDN)
- Location in the LDAP server where the record resides.

Most of the entries that you store in an LDAP server will have a name, and the name is frequently stored in the Common Name (cn) attribute. Because every object has a name, most objects you store in an LDAP will use their cn value as the basis for their RDN.

Search

A search operation is used to search the LDAP server. The client specifies the starting point (base DN) of the search, the search scope (either the object, its children, or the subtree rooted at the object), and a search filter.

For authorization requests, the search operation is directly performed without a bind operation. The LDAP server can be configured with certain privileges for the search operation to succeed. This privilege level is established with the bind operation.

An LDAP search operation can return multiple user entries for a specific user. In such cases, the LDAP client returns an appropriate error code to AAA. To avoid these errors, you must configure appropriate search filters to match a single entry.

Compare

The compare operation is used to replace a bind request with a compare request for an authentication. The compare operation helps to maintain the initial bind parameters for the connection.

LDAP Dynamic Attribute Mapping

The Lightweight Directory Access Protocol (LDAP) is a powerful and flexible protocol for communication with AAA servers. LDAP attribute maps provide a method to cross-reference the attributes retrieved from a server to Cisco attributes supported by the security appliances.

When a user authenticates a security appliance, the security appliance, in turn, authenticates the server and uses the LDAP protocol to retrieve the record for that user. The record consists of LDAP attributes associated with fields displayed on the user interface of the server. Each attribute retrieved includes a value that was entered by the administrator who updates the user records.

Prerequisite for Configuring SLDAP

If you are using a secure Transport Layer Security (TLS) secure connection, you must configure the X.509 certificates.

Restrictions for Configuring SLDAP

- LDAP referrals are not supported.
- Unsolicited messages or notifications from the LDAP server are not handled.
- LDAP authentication is not supported for interactive (terminal) sessions.

Configuring SLDAP

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
Step 4	**ipv4** *ipv4-address* **Example:** `Device(config-ldap-server)# ipv4 9.4.109.20`	Specifies the LDAP server IP address using IPv4.
Step 5	**timeout retransmit** *seconds* **Example:** `Device(config-ldap-server)# timeout retransmit 20`	Specifies the number of seconds the Cisco Catalyst 9800 Series Wireless Controller embedded wireless controller waits for a reply to an LDAP request before retransmitting the request.
Step 6	**bind authenticate root-dn password** [**0** *string* | **7** *string*] *string*	Specifies a shared secret text string used between the Cisco Catalyst 9800 Series

	Command or Action	Purpose
	Example: `Device(config-ldap-server)# bind authenticate root-dn CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345`	Wireless Controller embedded wireless controller and an LDAP server. Use the **0** line option to configure an unencrypted shared secret. Use the **7** line option to configure an encrypted shared secret.
Step 7	**base-dn** *string* **Example:** `Device(config-ldap-server)# base-dn CN=Users,DC=ca,DC=ssh2,DC=com`	Specifies the base Distinguished Name (DN) of the search.
Step 8	**mode secure** [**no- negotiation**] **Example:** `Device(config-ldap-server)# mode secure no- negotiation`	Configures LDAP to initiate the TLS connection and specifies the secure mode.
Step 9	**end** **Example:** `Device(config-ldap-server)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an AAA Server Group (GUI)

Configuring a device to use AAA server groups helps you to group existing server hosts, select a subset of the configured server hosts and use them for a particular service. A server group is used with a global server-host list. The server group lists the IP addresses of the selected server hosts.

You can create the following server groups:

Procedure

Step 1 RADIUS

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **RADIUS**.
b) Click the **Add** button. The **Create AAA Radius Server Group** dialog box appears.
c) Enter a name for the RADIUS server group in the **Name** field.
d) Choose a desired delimiter from the **MAC-Delimiter** drop-down list. The available options are colon, hyphen, and single-hyphen.
e) Choose a desired filter from the **MAC-Filtering** drop-down list. The available options are mac and Key.
f) Enter a value in the **Dead-Time (mins)** field to make a server non-operational. You must specify a value between 1 and 1440.
g) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the > button.
h) Click the **Save & Apply to Device** button.

Step 2 TACACS+

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **TACACS+**.
b) Click the **Add** button. The **Create AAA Tacacs Server Group** dialog box appears.
c) Enter a name for the TACACS server group in the **Name** field.
d) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the **>** button.
e) Click the **Save & Apply to Device** button.

Step 3 LDAP

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **LDAP**.
b) Click the **Add** button. The **Create AAA Ldap Server Group** dialog box appears.
c) Enter a name for the LDAP server group in the **Name** field.
d) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the **>** button.
e) Click the **Save & Apply to Device** button.

Configuring a AAA Server Group

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa group server ldap** *group-name* **Example:** `Device(config)# aaa group server ldap name1`	Defines the AAA server group with a group name and enters LDAP server group configuration mode. All members of a group must be of the same type, that is, RADIUS, LDAP, or TACACS+.
Step 5	**server** *name* **Example:** `Device(config-ldap-sg)# server server1`	Associates a particular LDAP server with the defined server group. Each security server is identified by its IP address and UDP port number.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-ldap-sg)# exit`	Exits LDAP server group configuration mode.

Configuring Search and Bind Operations for an Authentication Request

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
Step 5	**authentication bind-first** **Example:** `Device(config-ldap-server)# authentication bind-first`	Configures the sequence of search and bind operations for an authentication request.
Step 6	**authentication compare** **Example:** `Device(config-ldap-server)# authentication compare`	Replaces the bind request with the compare request for authentication.
Step 7	**exit** **Example:** `Device(config-ldap-server)# exit`	Exits LDAP server group configuration mode.

Configuring a Dynamic Attribute Map on an SLDAP Server

You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are compatible with the security appliance. You can then bind these attribute maps to LDAP servers or remove them as required.

Note To use the attribute mapping features correctly, you need to understand the Cisco LDAP and user-defined attribute names and values.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ldap attribute-map** *map-name* **Example:** `Device(config)# ldap attribute-map map1`	Configures a dynamic LDAP attribute map and enters attribute-map configuration mode.
Step 4	**map type** *ldap-attr-type aaa-attr-type* **Example:** `Device(config-attr-map)# map type department supplicant-group`	Defines an attribute map.
Step 5	**exit** **Example:** `Device(config-attr-map)# exit`	Exits attribute-map configuration mode.

Verifying the SLDAP Configuration

To view details about the default LDAP attribute mapping, use the following command:

```
Device# show ldap attributes
```

To view the LDAP server state information and various other counters for the server, use the following command:

```
Device# show ldap server
```

CHAPTER 113

Network Access Server Identifier

- Information About Network Access Server Identifier, on page 1233
- Creating a NAS ID Policy(GUI), on page 1234
- Creating a NAS ID Policy, on page 1234
- Attaching a Policy to a Tag (GUI), on page 1235
- Attaching a Policy to a Tag (CLI), on page 1235
- Verifying the NAS ID Configuration, on page 1236

Information About Network Access Server Identifier

Network access server identifier (NAS-ID) is used to notify the source of a RADIUS access request, which enables the RADIUS server to choose a policy for that request. You can configure one on each WLAN profile, VLAN interface, or access point group. The NAS-ID is sent to the RADIUS server by the controller through an authentication request to classify users to different groups. This enables the RADIUS server to send a customized authentication response.

Note The acct-session-id is sent with the RADIUS access request only when accounting is enabled on the policy profile.

If you configure a NAS-ID for an AP group, it overrides the NAS-ID that is configured for a WLAN profile or the VLAN interface. Similarly, if you configure a NAS-ID for a WLAN profile, it overrides the NAS-ID that is configured for the VLAN interface.

Starting with Cisco IOS XE Cupertino 17.7.1, a new string named custom-string (custom string) is added.

The following options can be configured for a NAS ID:

- sys-name (System Name)
- sys-ip (System IP Address)
- sys-mac (System MAC Address)
- ap-ip (AP's IP address)
- ap-name (AP's Name)
- ap-mac (AP's MAC Address)

- ap-eth-mac (AP's Ethernet MAC Address)
- ap-policy-tag (AP's policy tag name)
- ap-site-tag (AP's site tag name)
- ssid (SSID Name)
- ap-location (AP's Location)
- custom-string (custom string)

Creating a NAS ID Policy(GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless AAA Policy**.

Step 2 On the **Wireless AAA Policy** page, click the name of the **Policy** or click **Add** to create a new one.

Step 3 In the **Add/Edit Wireless AAA Policy** window that is displayed, enter the name of the policy in the **Policy Name** field.

Step 4 Choose from one of the NAS ID options from the **Option 1** drop-down list.

Step 5 Choose from one of the NAS ID options from the **Option 2** drop-down list.

Step 6 Choose from one of the NAS ID options from the **Option 3** drop-down list.

Step 7 Save the configuration.

Creating a NAS ID Policy

Follow the procedure given below to create NAS ID policy:

Before you begin

- NAS ID can be a combination of multiple NAS ID options; the maximum options are limited to 3.
- The maximum length of the NAS ID attribute is 253. Before adding a new attribute, the attribute buffer is checked, and if there is no sufficient space, the new attribute is ignored.
- By default, a wireless aaa policy (default-aaa-policy) is created with the default configuration (sys-name). You can update this policy with various NAS ID options. However, the default-aaa-policy cannot be deleted.
- If a NAS ID is not configured, the default sys-name is considered as the NAS ID for all wireless-specific RADIUS packets (authentication and accounting) from the controller .
- Starting with Cisco IOS XE Cupertino 17.7.1, you can configure a custom string with various combinations of option1, option2 and option3 (**nas-id option3 custom-string** *custom-string*) as NAS ID in RADIUS packets.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless aaa policy** *policy-name* **Example:** `Device(config)# wireless aaa policy test`	Configures a new AAA policy.
Step 3	**nas-id option1 sys-name** **Example:** `Device(config-aaa-policy)# nas-id option1 sys-name`	Configures NAS ID for option1.
Step 4	**nas-id option2 sys-ip** **Example:** `Device(config-aaa-policy)# nas-id option2 sys-ip`	Configures NAS ID for option2.
Step 5	**nas-id option3 sys-mac** **Example:** `Device(config-aaa-policy)# nas-id option3 sys-mac`	Configures NAS ID for option3.

Attaching a Policy to a Tag (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Tags** page, click **Policy** tab.
Step 2 Click **Add** to view the **Add Policy Tag** window.
Step 3 Enter a name and description for the policy tag.
Step 4 Click **Add** to map WLAN profile and Policy profile.
Step 5 Choose the **WLAN Profile** to map with the appropriate **Policy Profile**, and click the tick icon.
Step 6 Click **Save & Apply to Device**.

Attaching a Policy to a Tag (CLI)

Follow the procedure given below to attach a NAS ID policy to a tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy test1`	Configures a WLAN policy profile.
Step 3	**aaa-policy** *aaa-policy-name* **Example:** `Device(config-wireless-policy)# aaa-policy policy-aaa`	Configures a AAA policy profile.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 5	**wireless tag policy** *policy-tag* **Example:** `Device(config)# wireless tag policy policy-tag1`	Configures a wireless policy tag.
Step 6	**wlan wlan1 policy** *policy-name* **Example:** `Device(config)# wlan wlan1 policy test1`	Maps a WLAN profile to a policy profile. **Note** You can also use the **ap-tag** option to configure a NAS ID for an AP group, which will override the NAS ID that is configured for a WLAN profile or the VLAN interface.

Verifying the NAS ID Configuration

Use the following **show** command to verify the NAS ID configuration:

```
Device# show wireless profile policy detailed test1

Policy Profile Name           : test1
Description                   :
Status                        : ENABLED
VLAN                          : 1
Client count                  : 0

:
:
AAA Policy Params
```

```
AAA Override                : DISABLED
NAC                         : DISABLED
AAA Policy name             : test
```

CHAPTER 114

Locally Significant Certificates

- Information About Locally Significant Certificates, on page 1239
- Restrictions for Locally Significant Certificates, on page 1241
- Provisioning Locally Significant Certificates, on page 1242
- Verifying LSC Configuration, on page 1253
- Configuring Management Trustpoint to LSC (GUI), on page 1254
- Configuring Management Trustpoint to LSC (CLI), on page 1254
- Information About MIC and LSC Access Points Joining the Controller, on page 1255
- LSC Fallback Access Points, on page 1259
- Configuring Controller Self-Signed Certificate for Wireless AP Join, on page 1260

Information About Locally Significant Certificates

This module explains how to configure the Cisco Catalyst 9800 Series Wireless Controller and Lightweight Access Points (LAPs) to use the Locally Significant Certificate (LSC). If you choose the Public Key Infrastructure (PKI) with LSC, you can generate the LSC on the APs and controllers. You can then use the certificates to mutually authenticate the controllers and the APs.

In Cisco controllers, you can configure the controller to use an LSC. Use an LSC if you want your own PKI to provide better security, have control of your Certificate Authority (CA), and define policies, restrictions, and usages on the generated certificates.

You need to provision the new LSC certificate on the controller and then the Lightweight Access Point (LAP) from the CA Server.

The LAP communicates with the controller using the CAPWAP protocol. Any request to sign the certificate and issue the CA certificates for LAP and controller itself must be initiated from the controller. The LAP does not communicate directly with the CA server. The CA server details must be configured on the controller and must be accessible.

The controller makes use of the Simple Certificate Enrollment Protocol (SCEP) to forward certReqs generated on the devices to the CA and makes use of SCEP again to get the signed certificates from the CA.

The SCEP is a certificate management protocol that the PKI clients and CA servers use to support certificate enrollment and revocation. It is widely used in Cisco and supported by many CA servers. In SCEP, HTTP is used as the transport protocol for the PKI messages. The primary goal of SCEP is the secure issuance of certificates to network devices. SCEP is capable of many operations, but for our release, SCEP is utilized for the following operations:

- CA and Router Advertisement (RA) Public Key Distribution
- Certificate Enrollment

Certificate Provisioning in Controllers

The new LSC certificates, both CA and device certificates, must be installed on the controller.

With the help of SCEP, CA certificates are received from the CA server. During this point, there are no certificates in the controller. After the **get** operation of obtaining the CA certificates, are installed on the controller. The same CA certificates are also pushed to the APs when the APs are provisioned with LSCs.

Note We recommend that you use a new RSA keypair name for the newly configured PKI certificate. If you want to reuse an existing RSA keypair name (that is associated with an old certificate) for a new PKI certificate, do either of the following:

- Do not regenerate a new RSA keypair with an existing RSA keypair name, reuse the existing RSA keypair name. Regenerating a new RSA keypair with an existing RSA keypair name will make all the certificates associated with the existing RSA keypair invalid.
- Manually remove the old PKI certificate configurations first, before reusing the existing RSA keypair name for the new PKI certificate.

Device Certificate Enrollment Operation

For both the LAP and the controller that request a CA-signed certificate, the certRequest is sent as a PKCS#10 message. The certRequest contains the Subject Name, Public Key, and other attributes to be included in the X.509 certificate, and must be digitally signed by the Private Key of the requester. These are then sent to the CA, which transforms the certRequest into an X.509 certificate.

The CA that receives a PKCS#10 certRequest requires additional information to authenticate the requester's identity and verify if the request is unaltered. (Sometimes, PKCS#10 is combined with other approaches, such as PKCS#7 to send and receive the certificate request or response.)

The PKCS#10 is wrapped in a PKCS#7 Signed Data message type. This is supported as part of the SCEP client functionality, while the PKCSReq message is sent to the controller. Upon successful enrollment operation, both the CA and device certificates are available on the controller.

Certificate Provisioning on Lightweight Access Point

In order to provision a new certificate on LAP, while in CAPWAP mode, the LAP must be able to get the new signed X.509 certificate. In order to do this, it sends a certRequest to the controller, which acts as a CA proxy and helps obtain the certRequest signed by the CA for the LAP.

The certReq and the certResponses are sent to the LAP with the LWAPP payloads.

Both the LSC CA and the LAP device certificates are installed in the LAP, and the system reboots automatically. The next time when the system comes up, because it is configured to use LSCs, the AP sends the LSC device certificate to the controller as part of the JOIN Request. As part of the JOIN Response, the controller sends the new device certificate and also validates the inbound LAP certificate with the new CA root certificate.

What to Do Next

To configure, authorize, and manage certificate enrollment with the existing PKI infrastructure for controller and AP, you need to use the LSC provisioning functionality.

Restrictions for Locally Significant Certificates

- LSC workflow is different in FIPS+WLANCC mode. CA server must support Enrollment over Secure Transport (EST) protocol and should be capable of issuing EC certificates in FIPS+WLANCC mode.
- Elliptic Curve Digital Signature Algorithm (ECDSA) cipher works only if both AP and controller are having EC certificates, provisioned with LSC.
- EC certificates (LSC-EC) can be provisioned only if CA server supports EST (and not SCEP).
- FIPS + CC security modes is required to be configured in order to provision EC certificate.
- All AP misconfigurations should be corrected before enabling LSC. The count for misconfigured APs can be observed in the output of the following **show** command:

```
Device# show wireless summary
Priming controller         : DISABLED
Max APs supported          : 3000
Max clients supported      : 32000
Access Point Summary
                      Total    Up    Down
-----------------------------------------
802.11 2.4GHz             2     2       0
802.11 5GHz               5     2       3
802.11 6GHz               1     1       0
802.11 dual-band          2     0       2
802.11 dual-band(5/6GHz)  0     0       0
802.11 rx-dual-band       0     0       0
Client Serving(2.4GHz)    3     1       2
Client Serving(5GHz)      4     1       3
Client Serving(6GHz)      1     1       0
Monitor(Dual band)        0     0       0
Monitor(2.4GHz)           1     1       0
Monitor(5GHz)             1     1       0
Monitor(6GHz)             0     0       0
Sniffer(Dual band)        0     0       0
Sniffer(2.4GHz)           0     0       0
Sniffer(5GHz)             0     0       0
Sniffer(6GHz)             0     0       0
Misconfigured APs         1 (For more info use 'show ap tag summary')
Client Summary
  Total Clients : 0
  Excluded      : 0
  Disabled      : 0
  Foreign       : 0
  Anchor        : 0
  Local         : 0
```

For more information about misconfigured APs, run the **wireless config validate** command. To view reported errors, run the **show wireless config validation status** command.

Provisioning Locally Significant Certificates

Configuring RSA Key for PKI Trustpoint

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto key generate rsa** [**exportable**] **general-keys modulus** *key_size* **label** *RSA_key* **Example:** `Device(config)# crypto key generate rsa exportable general-keys modulus 2048 label lsc-tp`	Configures RSA key for PKI trustpoint. **exportable** is an optional keyword. You may or may not want to configure an exportable-key. If selected, you can export the key out of the box, if required • *key_size*: Size of the key modulus. The valid range is from 2048 to 4096. • *RSA_key*: RSA key pair label.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring PKI Trustpoint Parameters

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki trustpoint** *trustpoint_name* **Example:** `Device(config)# crypto pki trustpoint microsoft-ca`	Creates a new trustpoint for an external CA server. Here, *trustpoint_name* refers to the trustpoint name.
Step 3	**enrollment url** *HTTP_URL* **Example:**	Specifies the URL of the CA on which your router should send certificate requests.

	Command or Action	Purpose
	`Device(ca-trustpoint)# enrollment url http://CA_server/certsrv/mscep/mscep.dll`	**url** *url*: URL of the file system where your router should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: http://[2001:DB8:1:1::1]:80. For more enrollment method options, see the enrollment url (ca-trustpoint) command page.
Step 4	**subject-name** *subject_name* **Example:** `Device(ca-trustpoint)# subject-name C=IN, ST=KA, L=Bengaluru, O=Cisco, CN=eagle-eye/emailAddress=support@abc.com`	Creates subject name parameters for the trustpoint.
Step 5	**rsakeypair** *RSA_key key_size* **Example:** `Device(ca-trustpoint)# rsakeypair ewlc-tp1`	Maps RSA key with that of the trustpoint. • *RSA_key*: RSA key pair label. • *key_size*: Signature key length. Range is from 360 to 4096.
Step 6	**revocation** {**crl** | **none** | **ocsp**} **Example:** `Device(ca-trustpoint)# revocation none`	Checks revocation.
Step 7	**end** **Example:** `Device(ca-trustpoint)# end`	Returns to privileged EXEC mode.

Authenticating and Enrolling a PKI Trustpoint (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.

Step 2 In the **PKI Management** window, click the **Trustpoints** tab.

Step 3 In the **Add Trustpoint** dialog box, provide the following information:

a) In the **Label** field, enter the RSA key label.
b) In the **Enrollment URL** field, enter the enrollment URL.
c) Check the **Authenticate** check box to authenticate the Public Certificate from the enrollment URL.
d) In the **Subject Name** section, enter the **Country Code**, **State**, **Location**, **Organization**, **Domain Name**, and **Email Address**.
e) Check the **Key Generated** check box to view the available RSA keypairs. Choose an option from the **Available RSA Keypairs** drop-down list.
f) Check the **Enroll Trustpoint** check box.

g) In the **Password** field, enter the password.
h) In the **Re-Enter Password** field, confirm the password.
i) Click **Apply to Device**.

The new trustpoint is added to the trustpoint name list.

Authenticating and Enrolling the PKI Trustpoint with CA Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki authenticate** *trustpoint_name* **Example:** `Device(config)# crypto pki authenticate microsoft-ca`	Fetches the CA certificate.

Step 3	**yes**
	Example:
	`Device(config)# % Do you accept this certificate? [yes/no]:`
	`yes Trustpoint CA certificate accepted.`	

Step 4	**crypto pki enroll** *trustpoint_name*
	Example:
	`Device(config)# crypto pki enroll microsoft-ca`
	`%`
	`% Start certificate enrollment ..`
	`% Create a challenge password. You will need to verbally`
	`provide this password to the CA Administrator in order to`
	`revoke your certificate. For security reasons your password`
	`will not be saved in the configuration.`
	`Please make a note of it.`
		Enrolls the client certificate.

Step 5	**password** **Example:** `Device(config)# abcd123`	Enters a challenge password to the CA server.
Step 6	**password** **Example:** `Device(config)# abcd123`	Re-enters a challenge password to the CA server.

	Command or Action	Purpose
Step 7	**yes** **Example:** `Device(config)# % Include the router serial number in the subject name? [yes/no]: yes`	
Step 8	**no** **Example:** `Device(config)# % Include an IP address in the subject name? [no]: no`	
Step 9	**yes** **Example:** `Device(config)# Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose client' command will show the fingerprint.`	
Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring AP Join Attempts with LSC Certificate (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **All Access Points** window, click the LSC Provision name.

Step 3 From the **Status** drop-down list, choose a status to enable LSC.

Step 4 From the **Trustpoint Name** drop-down list, choose the trustpoint.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that will be permitted.

Step 6 Click **Apply**.

Configuring AP Join Attempts with LSC Certificate (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision join-attempt** *number_of_attempts* **Example:** `Device(config)# ap lsc-provision join-attempt 10`	Specifies the maximum number of AP join failure attempts with the newly provisioned LSC certificate. When the number of AP joins exceed the specified limit, AP joins back with the Manufacturer Installed Certificate (MIC).
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Subject-Name Parameters in LSC Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision subject-name-parameter country** *country-str* **state** *state-str* **city** *city-str* **domain** *domain-str* **org** *org-str* **email-address** *email-addr-str* **Example:** `Device(config)# ap lsc-provision subject-name-parameter country India state Karnataka city Bangalore domain domain1 org Right email-address adc@gfe.com`	Specifies the attributes to be included in the subject-name parameter of the certificate request generated by an AP.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring Key Size for LSC Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision key-size**{ **2048** | **3072** | **4096}**} **Example:** `Device(config)# ap lsc-provision key-size 2048`	Specifies the size of keys to be generated for the LSC on AP.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Trustpoint for LSC Provisioning on an Access Point

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision trustpoint** *tp-name* **Example:** `Device(config)# ap lsc-provision trustpoint microsoft-ca`	Specifies the trustpoint with which the LCS is provisioned to an AP. *tp-name*: The trustpoint name.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring an AP LSC Provision List (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **All Access Points** window, click the corresponding LSC Provision name.

Step 3 From the **Status** drop-down list, choose a status to enable LSC.

Step 4 From the **Trustpoint Name** drop-down list, choose a trustpoint.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that are allowed.

Step 6 From the **Key Size** drop-down list, choose a key.

Step 7 In the **Edit AP Join Profile** window, click the **CAPWAP** tab.

Step 8 In the **Add APs to LSC Provision List** section, click **Select File** to upload the CSV file that contains AP details.

Step 9 Click **Upload File**.

Step 10 In the **AP MAC Address** field, enter the AP MAC address. and add them. (The APs added to the provision list are displayed in the **APs in provision List** .)

Step 11 In the **Subject Name Parameters** section, enter the following details:

- **Country**
- **State**
- **City**
- **Organization**
- **Department**
- **Email Address**

Step 12 Click **Apply**.

Configuring an AP LSC Provision List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision mac-address** *mac-addr* **Example:** `Device(config)# ap lsc-provision mac-address 001b.3400.02f0`	Adds the AP to the LSC provision list. **Note** You can provision a list of APs using the **ap lsc-provision provision-list** command. (Or) You can provision all the APs using the **ap lsc-provision** command.

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring LSC Provisioning for all the APs (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Access Points** window, expand the **LSC Provision** section.

Step 3 Set **Status** to **Enabled** state.

Note If you set **Status** to **Provision List**, LSC provisioning will be configured only for APs that are a part of the provision list.

Step 4 From the **Trustpoint Name** drop-down list, choose the appropriate trustpoint for all APs.

Step 5 In the **Number of Join Attempts** field, enter the number of retry attempts that the APs can make to join the controller.

Step 6 From the **Key Size** drop-down list, choose the appropriate key size of the certificate:

- **2048**
- **3072**
- **4096**

Step 7 In the **Add APs to LSC Provision List** section, click **Select File** to upload the CSV file that contains the AP details.

Step 8 Click **Upload File**.

Step 9 In the **AP MAC Address** field, enter the AP MAC address. (The APs that are added to the provision list are displayed in the **APs in Provision List** section.)

Step 10 In the **Subject Name Parameters** section, enter the following details:

a. **Country**

b. **State**

c. **City**

d. **Organization**

e. **Department**

f. **Email Address**

Step 11 Click **Apply**.

Configuring LSC Provisioning for All APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision** **Example:** `Device(config)# ap lsc-provision`	Enables LSC provisioning for all APs. By default, LSC provisioning is disabled for all APs.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring LSC Provisioning for the APs in the Provision List

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision provision-list** **Example:** `Device(config)# ap lsc-provision provision-list`	Enables LSC provisioning for a set of APs configured in the provision list.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Importing a CA Certificate to the Trustpool (GUI)

PKI Trustpool Management is used to store a list of trusted certificates (either downloaded or built in) used by the different services on the controller. This is also used to authenticate a multilevel CA certificate. The built in CA certificate bundle in the PKI trustpool receives automatic updates from Cisco if they are not current, are corrupt, or if certain certificates need to be updated.

Perform this task to manually update the CA certificates in the PKI trustpool.

Note If your LSC has been issued by an intermediate CA, you must import the complete chain of CA certificates into the trustpool. Otherwise, you will not be able to provision the APs without the complete chain being present on the controller. The import step is not required if the certificate has been issued by a root CA.

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.

Step 2 In the **PKI Management** window, click the **Trustpool** tab.

Step 3 Click **Import**.

Step 4 In the **CA Certificate** field, copy and paste the CA certificate. Link together the multiple CA certificates in **.pem** format.

Step 5 Click **Apply to Device**.

Importing a CA Certificate to the Trustpool (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**crypto pki trust pool import terminal**
	Example:
	`Device(config)# crypto pki trust pool import terminal`
	`% Enter PEM-formatted CA certificate.`
	`% End with a blank line or "quit" on a line by itself.`
	`-----BEGIN CERTIFICATE-----`
	`-----END CERTIFICATE-----`
	`-----BEGIN CERTIFICATE-----`
	`-----END CERTIFICATE-----`
	`-----BEGIN CERTIFICATE-----`
	`-----END CERTIFICATE-----`
	`Aug 23 02:47:33.450:`
	`%PKI-6-TRUSTPOOL_DOWNLOAD_SUCCESS:`
	`Trustpool Download is successful`
		Imports the root certificate. For this, you need to paste the CA certificate from the **digicert.com**.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Cleaning the CA Certificates Imported in Trustpool (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.

Step 2 In the **PKI Management** window, click the **Trustpool** tab.

Step 3 Click **Clean**.

Note This erases the downloaded CA certificate bundles. However, it does not erase the built-in CA certificate bundles.

Step 4 Click **Yes**.

Cleaning CA Certificates Imported in Trustpool (CLI)

You cannot delete a specific CA certificate from the trustpool. However, you can clear all the CA certificates that are imported to the Trustpool.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto pki trustpool clean** **Example:** `Device(config)# crypto pki trustpool clean`	Erases the downloaded CA certificate bundles. However, it does not erase the built-in CA certificate bundles.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a New Trustpoint Dedicated to a Single CA Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**crypto pki trustpoint** *tp-name* **Example:** `Device(config)# crypto pki trustpoint tp_name`	Creates a trustpoint.
Step 3	**enrollment terminal** **Example:** `Device(ca-trustpoint)# enrollment terminal`	Creates an enrollment terminal for the trustpoint.
Step 4	**exit** **Example:** `Device(ca-trustpoint)# exit`	Exits from the truspoint configuration.

Step 5	**crypto pki authenticate** *tp-name*
	Example:
	`Device(config)# crypto pki authenticate tp_name`
	`<<< PASTE CA-CERT in PEM format followed by quit >>>`
		Authenticates the trustpoint.

Verifying LSC Configuration

To view the details of the wireless management trustpoint, use the following command:

```
Device# show wireless management trustpoint

Trustpoint  Name : microsoft-ca
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
 Private key Info : Available
```

To view the LSC provision-related configuration details for an AP, use the following command:

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : lsc-root-tp
Certificate chain status : Available
Number of certs on chain : 2
Certificate hash : 7f9d05183deecac4e5a79db65d538245685e8e30
LSC Revert Count in AP reboots : 1

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048
EC Key Size : 384 bit
```

```
AP LSC-provision List :

Total number of APs in provision list: 2

Mac Addresses :
--------------
1880.90f5.1540
2c5a.0f70.84dc
```

Configuring Management Trustpoint to LSC (GUI)

Procedure

Step 1 Choose **Administration** > **Management** > **HTTP/HTTPS**.

Step 2 In the **HTTP Trust Point Configuration** section, set **Enable Trust Point** to the **Enabled** state.

Step 3 From the **Trust Points** drop-down list, choose the appropriate trustpoint.

Step 4 Save the configuration.

Configuring Management Trustpoint to LSC (CLI)

After LSC provisioning, the APs will automatically reboot and join at the LSC mode after bootup. Similarly, if you remove the AP LSC provisioning, the APs reboot and join at non-LSC mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless management trustpoint** *trustpoint_name* **Example:** `Device(config)# wireless management trustpoint microsoft-ca`	Configures the management trustpoint to LSC.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Information About MIC and LSC Access Points Joining the Controller

Overview of Support for MIC and LSC Access Points Joining the Controller

In Cisco IOS XE Bengaluru 17.4.1 and earlier releases, APs with a default certificate (Manufacturing Installed Certificates [MIC]) or Secure Unique Device Identifier [SUDI]) fail to join a Locally Significant Certificate-deployed (LSC-deployed) controller, where the management certificate of the controller is an LSC. To resolve this issue, you must provision LSC on these APs using the provisioning controller before moving them to the LSC-deployed controller.

From Cisco IOS XE Bengaluru 17.5.1 onwards, the new authorization policy configuration allows MIC APs to join the LSC-deployed controller, so that the LSC and MIC APs can coexist in the controller at the same time.

Recommendations and Limitations

- When the CA server is configured with manual enrollment (manual intervention) to accept Certificate Signing Request (CSR), the controller waits for the CA server to send the pending response. If there is no response from the CA server for 10 minutes, the fallback mode comes into effect.
  - Cisco Wave 2 APs regenerate CSR, and a fresh CSR is sent to the CA server.
  - Cisco IOS APs restart, and then Cisco IOS APs send a fresh CSR, which is in turn sent to the CA server.
- Locally significant certificate (LSC) on the controller does not work on the password challenge. Therefore, for LSC to work, you must disable password challenge on the CA server.
- If you are using Microsoft CA, we recommend that you use Windows Server 2012 or later as the CA server.

Configuration Workflow

1. #unique_1615
2. #unique_1616
3. #unique_1617
4. #unique_1618

Configuring LSC on the Controller (CLI)

The server certificate used by the controller for CAPWAP-DTLS is based on the following configuration.

Before you begin

- Ensure that you enable LSC by setting the appropriate trustpoints for the following wireless management services:
  - AP join process: CAPWAP DTLS server certificate
  - Mobility connections: Mobility DTLS certificate
  - NMSP and CMX connections: NMSP TLS certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**[no] wireless management trustpoint** *trustpoint-name* **Example:** `Device(config)# wireless management trustpoint trustpoint-name`	Configures the LSC trustpoint in the LSC-deployed controller.

Enabling the AP Certificate Policy on the APs (CLI)

- If the management trustpoint is an LSC, by default, MIC APs fail to join the controller. This configuration acts as an enable or disable configuration knob that allows MIC APs to join the controller.
- This configuration is a controller authorization to allow APs to join MIC at the time of DTLS handshake.

To prevent manufacturing installed certificate (MIC) expiry failures, ensure that you configure a policy, as shown here:

- Create a certificate map and add the rules:

```
configure terminal
crypto pki certificate map map1 1
issuer-name co Cisco Manufacturing CA
```

Note You can add multiple rules and filters under the same map. The rule mentioned in the example above specifies that any certificate whose issuer-name contains *Cisco Manufacturing CA* (case insensitive) is selected under this map.

- Use the certificate map under the trustpool policy:

```
configure terminal
crypto pki trustpool policy
match certificate map1 allow expired-certificate
```

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap auth-list ap-cert-policy allow-mic-ap trustpoint** *trustpoint-name* **Example:** `Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint trustpoint-name`	Configures the trustpoint name for the controller certificate chain. **Note** The **allow-mic-ap trustpoint** command is required only for the virtual controller (Cisco Catalyst 9800-CL Wireless Controller for Cloud). In all the other appliance controller platforms, the default certificate is selected. This default certificate is manufacturer-installed SUDI.
Step 3	**ap auth-list ap-cert-policy allow-mic-ap** **Example:** `Device(config)# ap auth-list ap-cert-policy allow-mic-ap`	Enables the AP certificate policy during CAPWAP-DTLS handshake.
Step 4	**ap auth-list ap-cert-policy** {**mac-address** *H.H.H* | **serial-number** *serial-number-ap*} **policy-type mic** **Example:** `Device(config)# ap auth-list ap-cert-policy mac-address 1111.1111.1111 policy-type mic`	Enables the AP certificate policy as MIC.

Configuring the AP Policy Certificate (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Access Points**

Step 2 In the **All Access Points** window, click **AP Certificate Policy** .

Step 3 In the **AP Policy Certificate** window, complete the following actions:

a) Click the **Authorize APs joining with MIC** toggle button to enable AP authorization.

b) From the **Trustpoint Name** drop-down list, choose the required trustpoint.

c) Click **Add MAC or Serial Number** to add a MAC address or a serial number manually or through a .csv file.
The **Add MAC or Serial Number** window is displayed.

d) Click the **AP Authlist Type** and enter the MAC address or the serial number. Upload the .csv file or enter the MAC address in the list box.
The newly added MAC address and serial numbers are displayed under **List of MAC Address and Serial Numbers**.

e) Click **Apply**.

The AP certificate policy is added to the **AP Inventory** window.

Note To add a new AP with MIC, perform Step 1 to Step 3 described in Configuring the AP Policy Certificate (GUI) section. To add a new AP with LSC, perform the procedure described in the Configuring AP LSC Provision List (GUI) and Step 1 to Step 3 in the Configuring the AP Policy Certificate (GUI) section.

Configuring the Allowed List of APs to Join the Controller (CLI)

The allowed list of APs can either be populated based on the Ethernet MAC address or based on the serial number of the APs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap auth-list ap-cert-policy** {**mac-address** *AP-Ethernet-MAC-address* | **serial-number** *AP-serial-number*} **policy-type mic** **Example:** `Device# ap auth-list ap-cert-policy mac-address 00b0.e192.0d98 policy-type mic`	Configures the AP certificate policy based on the Ethernet MAC address or based on the assembly serial number of the AP.

Verifying the Configuration Status

To verify if the APs have been authorized by the AP certificate policy, use the following command:

```
Device# show ap auth-list ap-cert-policy
Authorize APs joining with MIC : ENABLED
MIC AP policy trustpoint
Name : CISCO_IDEVID_SUDI
Certificate status : Available
Certificate Type : MIC
Certificate Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

To verify the AP certificate policy on the MAC address and the serial number of the AP, use the following commands:

```
Device# show ap auth-list ap-cert-policy mac-address
MAC address      AP cert policy
---------------------------------
1111.2222.3333   MIC

Device# show ap auth-list ap-cert-policy serial-number
Serial number    AP cert policy
-------------------------------
F1234567890      MIC
```

Note If you set an invalid trustpoint (not SSC), the **allow-mic-ap policy** is not enabled. If you set an invalid trustpoint, the following error is displayed on the console:

```
Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint lsc-root-tp
Dec 18 07:38:29.944: %CERT_MGR_ERRMSG-3-CERT_MGR_GENERAL_ERR: Chassis 1 R0/0: wncd: General
 error: MIC AP Policy trustpoint: 'lsc-root-tp' cert-chain type is LSC, It must be either
MIC or vWLC-SSC
```

LSC Fallback Access Points

Information About LSC Fallback APs

When an AP is configured with LSC for CAPWAP but fails to establish DTLS connection, the AP reboots and retries for certain number of times. For information on how an AP configures with LSC, see Configuring AP Join Attempts with LSC Certificate (CLI), on page 1246.

The AP falls back to its default certificate (MIC) for CAPWAP after maximum number of failures. This state is referred to as the LSC fallback.

Note MIC is also known as SUDI certificate.

Troubleshooting LSC Fallback State

When an AP in **LSC fallback** state joins the controller, the following syslog is generated:

```
Jun 15 23:24:14.836: %APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/0: wncd: Error
in AP: 'AP2c5a.0f70.84dc' with address 70db.9888.cc20 is joined with MIC, while configuration

requires LSC. No WLANs will be pushed.
```

The controller allows such an AP to be joined with MIC (when AP certificate policy allows it) and AP is held in misconfigured state.

Note The AP does not broadcast WLAN or SSID configurations in such state. This permits the admin to examine the reason for previous failures and recover APs.

You can identify the **LSC fallback** APs using **show wireless summary** as follows:

```
Device# show wireless summary
…
Access Point Summary
…
DTLS LSC fallback APs     20 (No WLANs will be pushed to these APs)
…
For more information on DTLS LSC fallback APs,
    execute 'wireless config validate' and look for reported errors in
    'show wireless config validation status' CLI output.

Use 'show ap config general | inc AP Name | LSC fallback' to list DTLS LSC fallback APs.
Examine LSC fallback reasons / DTLS handshake failures with LSC then
    issue 'ap lsc dtls-fallback clear-certificate / clear-flag' to recover APs
```

Recovery Steps

- Use the **ap lsc dtls-fallback clear-flag** to clear the LSC fallback flag on AP and instruct AP to reload.

Note The AP reuses the LSC for CAPWAP DTLS connection post the reload.

- Use the **ap lsc dtls-fallback clear-certificate** to clear LSC and instruct AP to reload.

Note The AP uses MIC for CAPWAP-DTLS post the reload. If LSC is used for Dot1x port authentication then further recovery is needed on switch port for AP authentication.

Note

- The **ap lsc dtls-fallback clear-flag** command is sufficient to retain LSC on AP. Both **ap lsc dtls-fallback clear-flag** and **ap lsc dtls-fallback clear-certificate** commands are not required at the same time.
- APs must be in connected state when issuing the recovery command. You will need to reissue the command, if any **LSC fallback** AP joins afterwards.

Configuring Controller Self-Signed Certificate for Wireless AP Join

Use Cases

Use Case-1

Cisco Catalyst 9800-CL platform does not contain manufacturer installed SUDI certificates. You will need to configure Self-Signed Certificates on your controller.

Use Case-2

APs running on earlier versions and having Manufacturer Installed Certificate (MIC) issued by a SHA1 Cisco Trusted CA cannot join the controller with SHA2 SUDI certificate. During CAPWAP join process, the AP displays a bad certificate error and tears down the DTLS handshake.

Workaround: To upgrade APs, configure controller Self-Signed certificates. Once done, you can delete the Self-Signed certificates and revert back to the SUDI certificate.

Note This workaround does not apply to the Embedded Wireless Controller running Catalyst 9k switches. But applies to other hardware appliance controllers, such as Cisco Catalyst 9800-40, Cisco Catalyst 9800-80, and Cisco Catalyst 9800-L.

Note Certificate used in DTLS connections (AP and mobility) must use RSA key of size equal or more than 2048 bits. Otherwise, the APs and mobility connections will fail after reload. Run the **show crypto pki certificate verbose _tp-name_** command to display the key size of the device certificate.

Prerequisites

- Ensure that the VLAN interface is up and it's IP is reachable.
- Ensure that the **ip http server** is enabled. For more information, see Enabling HTTP Server.
- Set the **clock calendar-valid** command appropriately. For more information, see #unique_1633.
- Check if the PKI CA server is already configured or not. If configured, you will need to delete the existing CA server configuration.

Note The **show crypto pki server** command output should not display anything.

Configuring Clock Calendar (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**clock calendar-valid** **Example:** `Device(config)# clock calendar-valid`	Enables clock calendar.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Device(config)# exit`	Exits configuration mode.

Enabling HTTP Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. By default, the HTTP server uses the standard port 80.
Step 3	**ip http secure-server** **Example:** `Device(config)# ip http secure-server`	Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. By default, the HTTP server uses the standard port 80.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits configuration mode.

Configuring CA Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto key generate rsa general-keys modulus** *size_of_key_module* **label** *keypair_name* **Example:** `Device(config)# crypto key generate rsa general-keys modulus 2048 label WLC_CA`	Configures a certificate for the controller. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.

	Command or Action	Purpose
		Note The recommended key-pair name is *WLC_CA* and key modulus is *2048* bits.
Step 3	**crypto pki server** *certificate_server_name* **Example:** `Device(config)# crypto pki server WLC_CA`	Enables IOS certificate server. **Note** The *certificate_server_name* must be the same name as the *keypair_name*.
Step 4	**issuer-name** **Example:** `Device(config)# issuer-name O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC`	Configures X.509 distinguished name for the issuer CA certificate. **Note** You need to configure the same **issuer-name** as suggested for AP join.
Step 5	**grant auto** **Example:** `Device(config)# grant auto`	Grants certificate requests automatically.
Step 6	**hash sha256** **Example:** `Device(config)# hash sha256`	(Optional) Specifies the hash function for the signature used in the granted certificates.
Step 7	**lifetime ca-certificate** *time-interval* **Example:** `Device(config)# lifetime ca-certificate 3650`	(Optional) Specifies the lifetime in days of a CA certificate.
Step 8	**lifetime certificate** *time-interval* **Example:** `Device(config)# lifetime certificate 3650`	(Optional) Specifies the lifetime in days of a granted certificate.
Step 9	**database archive pkcs12 password** *password* **Example:** `Device(config)# database archive pkcs12 password 0 cisco123`	Sets the CA key and CA certificate archive format and password to encrypt the file.
Step 10	**no shutdown** **Example:** `Device(config)# no shutdown`	Enables the certificate server. **Note** Issue this command only after you have completely configured your certificate server.

	Command or Action	Purpose
Step 11	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Trustpoint (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto key generate rsa exportable general-keys modulus** *size-of-the-key-modulus* **label** *label* **Example:** `Device(config)# crypto key generate rsa exportable general-keys modulus 2048 label ewlc-tp1`	When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.
Step 3	**crypto pki trustpoint** *trustpoint_name* **Example:** `Device(config)# crypto pki trustpoint ewlc-tp1`	Creates a new trust point for an external CA server. Here, *trustpoint_name* refers to the trustpoint name. **Note** Ensure that same names are used for key-pair (*label*) and *trustpoint_name*.
Step 4	**rsakeypair** *RSA_key key_size* **Example:** `Device(ca-trustpoint)# rsakeypair ewlc-tp1`	Maps RSA key with that of the trustpoint. • RSA_key—Refers to the RSA key pair label. • key_size—Refers to the signature key length. The value ranges from 360 to 4096.
Step 5	**subject-name** *subject_name* **Example:** `Device(ca-trustpoint)# subject-name O=Cisco Virtual Wireless LAN Controller, CN=DEVICE-vWLC`	Creates subject name parameters for the trustpoint.
Step 6	**revocation-check none** **Example:**	Checks revocation.

	Command or Action	Purpose
	`Device(ca-trustpoint)# revocation-check none`	
Step 7	**hash sha256** **Example:** `Device(ca-trustpoint)# hash sha256`	Specifies the hash algorithm.
Step 8	**serial-number** **Example:** `Device(ca-trustpoint)# serial-number`	Specifies the serial number.
Step 9	**eku request server-auth client-auth** **Example:** `Device(ca-trustpoint)# eku request server-auth client-auth`	(Optional) Sets certificate key-usage purpose.
Step 10	**password** *password* **Example:** `Device(config)# password 0 cisco123`	Enables password.
Step 11	**enrollment url** *url* **Example:** `Device(config)# enrollment url http://<management-IPv4>:80`	Enrolls the URL. **Note** Replace the dummy IP with management VLAN interface IP of the controller where CA server is configured.
Step 12	**exit** **Example:** `Device(config)# exit`	Exits the configuration.

Authenticating and Enrolling the PKI TrustPoint with CA Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**crypto pki authenticate** *trustpoint_name*
	Example:
	`Device(config)# crypto pki authenticate ewlc-tp1`
	`Certificate has the following attributes:`
		Fetches the CA certificate.

	Command or Action	Purpose
	Fingerprint MD5: 64C5FC9A C581D827 C25FC3CF 1A7F42AC Fingerprint SHA1: 6FAFF812 7C552783 6A8FB566 52D95849 CC2FC050 % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted.	
Step 3	**crypto pki enroll** *trustpoint_name* **Example:** Device(config)# **crypto pki enroll ewlc-tp1** Enter following answers for UI interaction: % Include an IP address in the subject name? [no]: no Request certificate from CA? [yes/no]: yes	Enrolls for client certificate.
Step 4	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Tagging Wireless Management TrustPoint Name (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 2	**wireless management trustpoint** *trustpoint_name* **Example:** Device(config)# **wireless management trustpoint ewlc-tp1**	Tags the wireless management trustpoint name.
Step 3	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Controller Certificates for Wireless AP Join

To view the CA server details, use the following command:

```
Device# show crypto pki server
Certificate Server WLC_CA:
Status: enabled
State: enabled
Server's configuration is locked (enter "shut" to unlock it)
Issuer name: O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC
CA cert fingerprint: 79A3DBD5 59A7E384 73ABD152 C133F4E2
Granting mode is: auto
Last certificate issued serial number (hex): 1
CA certificate expiration timer: 12:04:00 UTC Mar 8 2029
CRL NextUpdate timer: 18:04:00 UTC Mar 11 2019
Current primary storage dir: nvram:
Database Level: Minimum - no cert data written to storage
```

To view the trustpoint details, use the following command:

```
Device# show crypto pki trustpoint ewlc-tp1 status
Trustpoint ewlc-tp1:
...
State:
Keys generated ..... Yes (General Purpose, exportable)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

To view the wireless management trustpoint details, use the following command:

```
Device# do show wireless management trustpoint
Trustpoint Name : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 4a5d777c5b2071c17faef376febc08398702184e
Private key Info : Available
FIPS suitability : Not Applicable
```

To view the HTTP server status, use the following command:

```
Device# show ip http server status | include server status
HTTP server status: Enabled
HTTP secure server status: Enabled
```

CHAPTER 115

Certificate Management

- About Public Key Infrastructure Management (GUI), on page 1269
- Authenticating and Enrolling a PKI Trustpoint (GUI), on page 1269
- Adding the Certificate Authority Server (GUI), on page 1270
- Adding an RSA or EC Key for PKI Trustpoint (GUI), on page 1271
- Adding and Managing Certificates , on page 1271

About Public Key Infrastructure Management (GUI)

The Public Key Infrastructure (PKI) Management page displays the following tabs:

Trustpoints tab: Used to add, create or enroll a new trustpoint. This page also displays the current trustpoints configured on the controller and other details of the trustpoint. You can also view if the trustpoint is in use for any of the features. For example, Webadmin or AP join (Wireless Management Interface), and others.

CA Server tab: Used to enable or disable the Certificate Authority (CA) server functionality on the controller. The CA server functionality should be enabled for the controller to generate a Self Signed Certificate (SSC).

Key Pair Generation tab: Used to generate key pairs.

Certificate Management tab: Used to generate and manage certificates, and perform all certificate related operations, on the controller.

Authenticating and Enrolling a PKI Trustpoint (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.

Step 2 In the **PKI Management** window, click the **Trustpoints** tab.

Step 3 In the **Add Trustpoint** dialog box, provide the following information:

a) In the **Label** field, enter the RSA key label.

b) In the **Enrollment URL** field, enter the enrollment URL.

c) Check the **Authenticate** check box to authenticate the Public Certificate from the enrollment URL.

d) In the **Subject Name** section, enter the **Country Code**, **State**, **Location**, **Organization**, **Domain Name**, and **Email Address**.
e) Check the **Key Generated** check box to view the available RSA keypairs. Choose an option from the **Available RSA Keypairs** drop-down list.
f) Check the **Enroll Trustpoint** check box.
g) In the **Password** field, enter the password.
h) In the **Re-Enter Password** field, confirm the password.
i) Click **Apply to Device**.

The new trustpoint is added to the trustpoint name list.

Generating an AP Self-Signed Certificate (GUI)

Note This section is valid only for virtual controllers (Cisco Catalyst 9800-CL Wireless Controller for Cloud) and not applicable for appliance based controllers (Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-80 Wireless Controller, Cisco Catalyst 9800-L Wireless Controller (Copper Uplink), and Cisco Catalyst 9800-L Wireless Controller (Fiber Uplink)).

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.
Step 2 In the **AP SSC Trustpoint** area, click **Generate** to generate an AP SSC trustpoint.
Step 3 From the **RSA Key-Size** drop-down list, choose a key size.
Step 4 From the **Signature Algorithm** drop-down list, choose an option.
Step 5 From the **Password Type** drop-down list, choose a password type.
Step 6 In the **Password** field, enter a password. The valid range is between 8 and 32 characters.
Step 7 Click **Apply to Device**.

Adding the Certificate Authority Server (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.
Step 2 In the **PKI Management** window, click the **CA Server** tab.
Step 3 In the **CA Server** section, click the **Shutdown Status** toggle button, to enable the status. If you choose the shutdown status as **Enabled**, you must enter the password and confirm the same.
Step 4 If you choose the shutdown status as **Disabled**, you must enter the **Country Code**, **State**, **Location**, **Organization**, **Domain Name**, and **Email Address**.

Step 5 Click **Apply** to add the CA server.

Step 6 Click **Remove CA Server** to delete the CA server.

Adding an RSA or EC Key for PKI Trustpoint (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management**.

Step 2 In the **PKI Management** window, click the **Key Pair Generation** tab.

Step 3 In the **Key Pair Generation** section, click **Add**.

Step 4 In the dialog box that is displayed, provide the following information:

a) In the **Key Name** field, enter the key name.

b) In the **Key Type** options, select either **RSA Key** or **EC Key**.

c) In the **Modulus Size** field, enter the modulus value for the RSA key or the EC key. The default modulus size for the RSA key is 4096 and the default value for the EC key is 521.

d) Check the **Key Exportable** check box to export the key. By default, this is checked.

e) Click **Generate**.

Adding and Managing Certificates

To add and manage certificates, use one of the following methods:

Note While configuring a password for the .pfx file, do not use the following ASCII characters: "*, ^, (), [], \, ", and +"

Using these ASCII characters results in error with bad configuration and does not import the certificate to the controller.

Method 1

Procedure

Step 1 Choose **Configuration** > **Security** > **PKI Management** > **Add Certificate**.

Step 2 Click **Generate Certificate Signing Request**.

a) In the **Certificate Name** field, enter the certificate name.

b) From the **Key Name** drop-down list, choose an RSA key pair. (Click the plus (+) icon under the **Key Pair Generation** tab to create new RSA key pairs.).

c) Enter values the **Country Code**, **Location**, **Organization**, **State**, **Organizational Unit**, and the **Domain Name** fields.

d) Click **Generate**.
The generated Certificate Signing Request (CSR) is displayed on the right. Click **Copy** to copy and save a local copy. Click **Save to Device** to save the generated CSR to the /bootflash/csr directory.

Step 3 Click **Authenticate Root CA** .

a) From the **Trustpoint** drop-down list, choose the trustpoint label generated in Step 2, or any other trustpoint label that you want to authenticate.

b) In the **Root CA Certificate (.pem)** field, copy and paste the certificate that you have received from the CA.

Note Ensure that you copy and paste the PEM Base64 certificate of the issuing CA of the device certificate.

c) Click **Authenticate**.

Step 4 Click **Import Device Certificate** .

a) From the **Trustpoint** drop-down list, choose the trustpoint label that was generated in Step 2, or any other trustpoint label that you want to authenticate.

b) In the **Signed Certificate (.pem)** field, copy and paste the signed certificate that you received, from your CA.

c) Click **Import**.

This completes the device certificate import process and the certificate can now be assigned to features.

Method 2

Procedure

Click **Import PKCS12 Certificate** .

Note You can import an entire certificate chain in the PKCS12 format using different transport types.

a) From the **Transport Type** drop-down list, choose either **FTP**, **SFTP**, **TFTP**, **SCP**, or **Desktop (HTTPS)**.

For **FTP**, **SFTP**, and **SCP**, enter values in the **Server IP Address (IPv4/IPv6)**, **Username**, **Password**, **Certificate File Path**, **Certificate Destination File Name**, and **Certificate Password** fields.

For **TFTP**, enter values in the **Server IP Address (IPv4/IPv6)**, **Certificate File Path**, **Certificate Destination File Name**, and **Certificate Password** fields.

For **Desktop (HTTPS)**, enter values in the **Source File Path** and **Certificate Password** fields.

b) Click **Import**.

CHAPTER 116

Controller Self-Signed Certificate for Wireless AP Join

- Use Cases, on page 1273
- Prerequisites, on page 1274
- Configuring Clock Calendar (CLI), on page 1274
- Enabling HTTP Server (CLI), on page 1275
- Configuring CA Server (CLI), on page 1275
- Configuring Trustpoint (CLI), on page 1277
- Authenticating and Enrolling the PKI TrustPoint with CA Server (CLI), on page 1278
- Tagging Wireless Management TrustPoint Name (CLI), on page 1279
- Verifying Controller Certificates for Wireless AP Join, on page 1279

Use Cases

Use Case-1

Cisco Catalyst 9800-CL platform does not contain manufacturer installed SUDI certificates. You will need to configure Self-Signed Certificates on your controller.

Use Case-2

APs running on earlier versions and having Manufacturer Installed Certificate (MIC) issued by a SHA1 Cisco Trusted CA cannot join the controller with SHA2 SUDI certificate. During CAPWAP join process, the AP displays a bad certificate error and tears down the DTLS handshake.

Workaround: To upgrade APs, configure controller Self-Signed certificates. Once done, you can delete the Self-Signed certificates and revert back to the SUDI certificate.

Note This workaround does not apply to the Embedded Wireless Controller running Catalyst 9k switches. But applies to other hardware appliance controllers, such as Cisco Catalyst 9800-40, Cisco Catalyst 9800-80, and Cisco Catalyst 9800-L.

Note Certificate used in DTLS connections (AP and mobility) must use RSA key of size equal or more than 2048 bits. Otherwise, the APs and mobility connections will fail after reload. Run the **show crypto pki certificate verbose _tp-name_** command to display the key size of the device certificate.

Prerequisites

- Ensure that the VLAN interface is up and it's IP is reachable.
- Ensure that the **ip http server** is enabled. For more information, see Enabling HTTP Server.
- Set the **clock calendar-valid** command appropriately. For more information, see #unique_1633.
- Check if the PKI CA server is already configured or not. If configured, you will need to delete the existing CA server configuration.

Note The **show crypto pki server** command output should not display anything.

Configuring Clock Calendar (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**clock calendar-valid** **Example:** `Device(config)# clock calendar-valid`	Enables clock calendar.
Step 3	**exit** **Example:** `Device(config)# exit`	Exits configuration mode.

Enabling HTTP Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. By default, the HTTP server uses the standard port 80.
Step 3	**ip http secure-server** **Example:** `Device(config)# ip http secure-server`	Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. By default, the HTTP server uses the standard port 80.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits configuration mode.

Configuring CA Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto key generate rsa general-keys modulus** *size_of_key_module* **label** *keypair_name* **Example:** `Device(config)# crypto key generate rsa general-keys modulus 2048 label WLC_CA`	Configures a certificate for the controller. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use. **Note** The recommended key-pair name is *WLC_CA* and key modulus is *2048* bits.
Step 3	**crypto pki server** *certificate_server_name*	Enables IOS certificate server.

	Command or Action	Purpose
	Example: `Device(config)# crypto pki server WLC_CA`	**Note** The *certificate_server_name* must be the same name as the *keypair_name*.
Step 4	**issuer-name** **Example:** `Device(config)# issuer-name O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC`	Configures X.509 distinguished name for the issuer CA certificate. **Note** You need to configure the same **issuer-name** as suggested for AP join.
Step 5	**grant auto** **Example:** `Device(config)# grant auto`	Grants certificate requests automatically.
Step 6	**hash sha256** **Example:** `Device(config)# hash sha256`	(Optional) Specifies the hash function for the signature used in the granted certificates.
Step 7	**lifetime ca-certificate** *time-interval* **Example:** `Device(config)# lifetime ca-certificate 3650`	(Optional) Specifies the lifetime in days of a CA certificate.
Step 8	**lifetime certificate** *time-interval* **Example:** `Device(config)# lifetime certificate 3650`	(Optional) Specifies the lifetime in days of a granted certificate.
Step 9	**database archive pkcs12 password** *password* **Example:** `Device(config)# database archive pkcs12 password 0 cisco123`	Sets the CA key and CA certificate archive format and password to encrypt the file.
Step 10	**no shutdown** **Example:** `Device(config)# no shutdown`	Enables the certificate server. **Note** Issue this command only after you have completely configured your certificate server.
Step 11	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Trustpoint (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto key generate rsa exportable general-keys modulus** *size-of-the-key-modulus* **label** *label* **Example:** `Device(config)# crypto key generate rsa exportable general-keys modulus 2048 label ewlc-tp1`	When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.
Step 3	**crypto pki trustpoint** *trustpoint_name* **Example:** `Device(config)# crypto pki trustpoint ewlc-tp1`	Creates a new trust point for an external CA server. Here, *trustpoint_name* refers to the trustpoint name. **Note** Ensure that same names are used for key-pair (*label*) and *trustpoint_name*.
Step 4	**rsakeypair** *RSA_key key_size* **Example:** `Device(ca-trustpoint)# rsakeypair ewlc-tp1`	Maps RSA key with that of the trustpoint. • RSA_key—Refers to the RSA key pair label. • key_size—Refers to the signature key length. The value ranges from 360 to 4096.
Step 5	**subject-name** *subject_name* **Example:** `Device(ca-trustpoint)# subject-name O=Cisco Virtual Wireless LAN Controller, CN=DEVICE-vWLC`	Creates subject name parameters for the trustpoint.
Step 6	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	Checks revocation.
Step 7	**hash sha256** **Example:** `Device(ca-trustpoint)# hash sha256`	Specifies the hash algorithm.

	Command or Action	Purpose
Step 8	**serial-number** **Example:** `Device(ca-trustpoint)# serial-number`	Specifies the serial number.
Step 9	**eku request server-auth client-auth** **Example:** `Device(ca-trustpoint)# eku request server-auth client-auth`	(Optional) Sets certificate key-usage purpose.
Step 10	**password** *password* **Example:** `Device(config)# password 0 cisco123`	Enables password.
Step 11	**enrollment url** *url* **Example:** `Device(config)# enrollment url http://<management-IPv4>:80`	Enrolls the URL. **Note** Replace the dummy IP with management VLAN interface IP of the controller where CA server is configured.
Step 12	**exit** **Example:** `Device(config)# exit`	Exits the configuration.

Authenticating and Enrolling the PKI TrustPoint with CA Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**crypto pki authenticate** *trustpoint_name*
	Example:
	`Device(config)# crypto pki authenticate ewlc-tp1`
	`Certificate has the following attributes:`
	`Fingerprint MD5: 64C5FC9A C581D827 C25FC3CF 1A7F42AC`
	`Fingerprint SHA1: 6FAFF812 7C552783 6A8FB566 52D95849 CC2FC050`
	`% Do you accept this certificate?`
		Fetches the CA certificate.

	Command or Action	Purpose
	`[yes/no]: yes` `Trustpoint CA certificate accepted.`	

Step 3	**crypto pki enroll** *trustpoint_name*
	Example:
	`Device(config)# crypto pki enroll ewlc-tp1`
	`Enter following answers for UI interaction:`
	`% Include an IP address in the subject name? [no]: no`
	`Request certificate from CA? [yes/no]: yes`
		Enrolls for client certificate.

Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Tagging Wireless Management TrustPoint Name (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless management trustpoint** *trustpoint_name* **Example:** `Device(config)# wireless management trustpoint ewlc-tp1`	Tags the wireless management trustpoint name.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Controller Certificates for Wireless AP Join

To view the CA server details, use the following command:

```
Device# show crypto pki server
Certificate Server WLC_CA:
Status: enabled
```

```
State: enabled
Server's configuration is locked (enter "shut" to unlock it)
Issuer name: O=Cisco Virtual Wireless LAN Controller, CN=CA-vWLC
CA cert fingerprint: 79A3DBD5 59A7E384 73ABD152 C133F4E2
Granting mode is: auto
Last certificate issued serial number (hex): 1
CA certificate expiration timer: 12:04:00 UTC Mar 8 2029
CRL NextUpdate timer: 18:04:00 UTC Mar 11 2019
Current primary storage dir: nvram:
Database Level: Minimum - no cert data written to storage
```

To view the trustpoint details, use the following command:

```
Device# show crypto pki trustpoint ewlc-tp1 status
Trustpoint ewlc-tp1:
...
State:
Keys generated ..... Yes (General Purpose, exportable)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

To view the wireless management trustpoint details, use the following command:

```
Device# do show wireless management trustpoint
Trustpoint Name : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 4a5d777c5b2071c17faef376febc08398702184e
Private key Info : Available
FIPS suitability : Not Applicable
```

To view the HTTP server status, use the following command:

```
Device# show ip http server status | include server status
HTTP server status: Enabled
HTTP secure server status: Enabled
```

CHAPTER 117

Managing Rogue Devices

- Rogue Detection, on page 1281
- Rogue Detection Security Level, on page 1293
- Setting Rogue Detection Security-level , on page 1294
- Wireless Service Assurance Rogue Events, on page 1295
- Rogue Full Scale Quotas and Priorities, on page 1296

Rogue Detection

Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. There is an increased chance of enterprise security breach when wireless users connect to access points in the enterprise network.

The following are some guidelines to manage rogue devices:

- The access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to detect a large number of rogue APs and clients with high sensitivity, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point continues to spend about 50 milliseconds on each channel.

- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect many rogue devices.
- Client card implementation might mitigate the effectiveness of containment. This normally happens when a client might quickly reconnect to the network after receiving a "de-association/de-authentication" frame, so it might still be able to pass some traffic. However, the browsing experience of the rogue client would be badly affected when it is contained.
- It is possible to classify and report rogue access points by using rogue states and user-defined classification rules that enable rogues to automatically move between states.
- Each controller limits the number of rogue containments to three and six per radio for access points in the monitor mode.
- When manual containment is performed using configuration, the rogue entry is retained even after the rogue entry expires.
- When a rogue entry expires, the managed access points are instructed to stop any active containment on it.
- When Validate Rogue AP Against AAA is enabled, the controller requests the AAA server for rogue AP classification with the configured interval.
- To validate a Rogue AP against AAA, add the rogue AP MAC to the AAA user-database with relevant delimiter, username, and password being the MAC address with relevant delimiter. The Access-Accept contains the Cisco-AV-pair with one of the following keywords:
  - **rogue-ap-state**=*state*

Note Here, **state** can be either of the types, namely: alert, contain, internal, external, or threat.

  - **rogue-ap-class**=*class*

Note Here, **class** can be either of the types, namely: unclassified, malicious, or friendly.

  The following are the allowed combinations of class or state:
  - **unclassified**: alert, contain, or threat.
  - **malicious**: alert, contain, or threat.
  - **friendly**: alert, internal, or external.

  The Radius Access-Reject for rogue AP AAA validation is ignored.
- When Validate Rogue Clients Against AAA is enabled, the controller requests the AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling Validate Rogue Clients Against AAA.

Restrictions on Rogue Detection

- Rogue containment is not supported on DFS channels.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.
- Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

From 17.7.1 release onwards, Beacon DS Attack and Beacon Wrong Channel signatures were introduced.

Beacon DS Attack—When managed and rogue APs use the same BSSID, the rogue APs are termed as impersonators. An attacker can add the Direct-Sequence parameter set information element with any channel number. If the added channel number is different from the channel number used by the managed AP, the attack is termed as Beacon DS Attack.

Beacon Wrong Channel—When managed and rogue APs use the same BSSID, the rogue APs are termed as AP impersonators. If an AP impersonator uses a channel number that is different from the one used by the managed AP with the same BSSID, the attack is termed as Beacon Wrong Channel. In such a case, the Direct-Sequence Information Element might not even be present in the Beacon frame.

Cisco Prime Infrastructure Interaction and Rogue Detection

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:

- If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.
- If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points that are categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

Information About Rogue Containment (Protected Management Frames (PMF) Enabled)

From Cisco IOS XE Amsterdam, 17.3.1 onwards, rogue devices that are enabled with 802.11w Protected Management Frames (PMF) are not contained. Instead, the rogue device is marked as *Contained Pending*, and a WSA alarm is raised to inform about the Contained Pending event. Because the device containment is not performed, access point (AP) resources are not consumed unnecessarily.

Note This feature is supported only on the Wave 2 APs.

Run the **show wireless wps rogue ap detailed** command to verify the device containment, when PMF is enabled on a rogue device.

AP Impersonation Detection

The various methods to detect AP impersonation are:

- AP impersonation can be detected if a managed AP reports itself as Rogue. This method is always enabled and no configuration is required.
- AP impersonation detection is based on MFP.
- AP impersonation detection based on AP authentication.

Infrastructure MFP protects 802.11 session management functions by adding message integrity check (MIC) information elements, to the management frames sent by APs (and not those sent by clients), which are then validated by other APs in the network. If infrastructure MFP is enabled, the managed APs check if the MIC information elements are present and if MIC information elements are as expected. If either of these conditions is not fulfilled, the managed AP sends rogue AP reports with updated AP authentication failure counter.

The AP Authentication functionality allows you to detect AP impersonation. When you enable this functionality, the controller creates an AP domain secret and shares it with other APs in the same network. This allows the APs to authenticate each other.

An AP Authentication information element is attached to beacon and probe response frames. If the AP Authentication information element has an incorrect Signature field, or the timestamp is off, or if the AP Authentication information element is missing, then the AP that has detected such a condition increments the **AP authentication failure count** field. An impersonation alarm is raised after the **AP authentication failure count** field breaches its threshold. The rogue AP is classified as **Malicious** with state **Threat**.

Run the **show wireless wps rogue ap detail** command to see when the impersonation is detected due to authentication errors.

Note Ensure that the **ccx aironet-iesupport** command is run in all the WLAN procedures, else the BSSID will be detected as a rogue.

For AP impersonation detection, Network Time Protocol (NTP) must be enabled instead of CAPWAP based time, under the AP profile.

Configuring Rogue Detection (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click the **AP Join Profile Name** to edit the AP join profile properties.

Step 3 In the **Edit AP Join Profile** window, click the **Rogue AP** tab.

Step 4 Check the **Rogue Detection** check box to enable rogue detection.

Step 5 In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

Step 6 In the **Rogue Detection Transient Interval** field, enter the interval in seconds.

Step 7 In the **Rogue Detection Report Interval** field, enter the report interval value in seconds.

Step 8 In the **Rogue Detection Client Number Threshold** field, enter the threshold for rogue client detection.

Step 9 Check the **Auto Containment on FlexConnect Standalone** check box to enable auto containment.

Step 10 Click **Update & Apply to Device**.

Configuring Rogue Detection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ap profile** *profile-name* **rogue detection min-rssi** *rssi in dBm*
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection min-rssi -100`
		Specify the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the device.
		Valid range for the rssi in dBm parameter is –128 dBm to -70 dBm, and the default value is -128 dBm.
		Note This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.

Step 3	**ap profile** *profile-name* **rogue detection containment** {**auto-rate** | **flex-rate**}
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection containment flex-rate`
		Specifies the rogue containment options. The **auto-rate** option enables auto-rate for containment of rogues. The **flex-rate** option enables rogue containment of standalone FlexConnect APs.

Step 4	**ap profile** *profile-name* **rogue detection enable**
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection enable`
		Enables rogue detection on all APs.

	Command or Action	Purpose

Step 5	**ap profile** *profile-name* **rogue detection report-interval** *time in seconds*
	Example:
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection report-interval 120`
		Configures rogue report interval for monitor mode Cisco APs.
		The valid range for reporting the interval in seconds is 10 seconds to 300 seconds.

Configuring RSSI Deviation Notification Threshold for Rogue APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue ap notify-rssi-deviation** **Example:** `Device(config)# wireless wps rogue ap notify-rssi-deviation`	Configures RSSI deviation notification threshold for Rogue APs.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Management Frame Protection (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies**.

Step 2 In the **Rogue Policy** tab, under the **MFP Configuration** section, check the **Global MFP State** check box and the **AP Impersonation Detection** check box to enable the global MFP state and the AP impersonation detection, respectively.

Step 3 In the **MFP Key Refresh Interval** field, specify the refresh interval in hours.

Step 4 Click **Apply**.

Configuring Management Frame Protection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps mfp** **Example:** `Device(config)# wireless wps mfp`	Configures a management frame protection.

Step 3	**wireless wps mfp** {**ap-impersonation** | **key-refresh-interval**}
	Example:
	`Device(config)# wireless wps mfp ap-impersonation`
	`Device(config)# wireless wps mfp key-refresh-interval`
		Configures ap impersonation detection (or) MFP key refresh interval in hours.
		key-refresh-interval—Refers to the MFP key refresh interval in hours. The valid range is from 1 to 24. Default value is 24.

Step 4	**end** **Example:** `Device(config)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Enabling Access Point Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps ap-authentication** **Example:** `Device(config)# wireless wps ap-authentication`	Configures the wireless WPS AP authentication.
Step 3	**wireless wps ap-authentication threshold** *threshold* **Example:** `Device(config)# wireless wps ap-authentication threshold 100`	Configures AP neighbor authentication and sets the threshold for AP authentication failures.

	Command or Action	Purpose
Step 4	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Configures a WLAN.
Step 5	**ccx aironet-iesupport** **Example:** `Device(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet Information Elements on this WLAN.
Step 6	**end** **Example:** `Device# end`	Returns to privileged EXEC mode.

Verifying Management Frame Protection

To verify if the Management Frame Protection (MFP) feature is enabled or not, use the following command:

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

To view the MFP details, use the following command:

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

Verifying Rogue Events

To verify the rogue event history, run the **show wireless wps rogue ap detailed** command:

```
Device# show wireless wps rogue ap detailed
Rogue Event history

Timestamp                  #Times   Class/State Event                Ctx
     RC
-------------------------- -------- ----------- -------------------- -------------------------
 ----
05/10/2021 13:56:46.657434 2        Mal/Threat  FSM_GOTO
Threat  0x0
```

```
05/10/2021 13:56:46.654905 1        Unk/Init    EXPIRE_TIMER_START
240s  0x0
05/10/2021 13:56:46.654879 1       Unk/Init    AP_IMPERSONATION          DS:1,ch:1,band_id:0
  0x0
05/10/2021 13:56:46.654673 1       Unk/Init    RECV_REPORT                  70db.98fc.2680/0
  0x0
05/10/2021 13:56:46.654663 1        Unk/Init    INIT_TIMER_START
180s  0x0
05/10/2021 13:56:46.654608 1        Unk/Init    CREATE
      0x0
```

```
Rogue BSSID                          : 002c.c8c1.096d
Last heard Rogue SSID                : MarvellAP0d
802.11w PMF required                 : No
Is Rogue an impersonator             : Yes
Beacon Wrong Channel                 : Yes
Beacon DS Attack                     : Yes
Is Rogue on Wired Network            : No
Classification                       : Malicious
Manually Contained                   : No
State                                : Threat
First Time Rogue was Reported        : 05/10/2021 13:56:46
Last Time Rogue was Reported         : 05/10/2021 13:56:46

Number of clients                    : 0
```

Verifying Rogue Detection

This section describes the new command for rogue detection.

The following command can be used to verify rogue detection on the device.

Table 80: Verifying Adhoc Rogues Information

Command	Purpose
show wireless wps rogue adhoc detailed *mac_address*	Displays the detailed information for an Adhoc rogue.
show wireless wps rogue adhoc summary	Displays a list of all Adhoc rogues.

Table 81: Verifying Rogue AP Information

Command	Purpose
show wireless wps rogue ap clients *mac_address*	Displays the list of all rogue clients associated with a rogue.
show wireless wps rogue ap custom summary	Displays the custom rogue AP information.
show wireless wps rogue ap detailed *mac_address*	Displays the detailed information for a rogue AP.
show wireless wps rogue ap friendly summary	Displays the friendly rogue AP information.
show wireless wps rogue ap list *mac_address*	Displays the list of rogue APs detected by a given AP.
show wireless wps rogue ap malicious summary	Displays the malicious rogue AP information.

show wireless wps rogue ap summary	Displays a list of all Rogue APs.
show wireless wps rogue ap unclassified summary	Displays the unclassified rogue AP information.

Table 82: Verifying Rogue Auto-Containment Information

Command	Purpose
show wireless wps rogue auto-contain	Displays the rogue auto-containment information.

Table 83: Verifying Classification Rule Information

Command	Purpose
show wireless wps rogue rule detailed *rule_name*	Displays the detailed information for a classification rule.
show wireless wps rogue rule summary	Displays the list of all rogue rules.

Table 84: Verifying Rogue Statistics

Command	Purpose
show wireless wps rogue stats	Displays the rogue statistics.

Table 85: Verifying Rogue Client Information

Command	Purpose
show wireless wps rogue client detailed *mac_address*	Displays detailed information for a Rogue client.
show wireless wps rogue client summary	Displays a list of all the Rogue clients.

Table 86: Verifying Rogue Ignore List

Command	Purpose
show wireless wps rogue ignore-list	Displays the rogue ignore list.

Examples: Rogue Detection Configuration

This example shows how to configure the minimum RSSI that a detected rogue AP needs to be at, to have an entry created in the device:

```
Device# configure terminal
Device(config)# ap profile profile1
Device(config)# rogue detection min-rssi -100
```

```
Device(config)# end
Device# show wireless wps rogue client summary/show wireless wps rogue ap summary
```

This example shows how to configure the classification interval:

```
Device# configure terminal
Device(config)# ap profile profile1
Device(config)# rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client summary/show wireless wps rogue ap summary
```

Configuring Rogue Policies (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies**.

Step 2 In the **Rogue Policies** tab, use the **Rogue Detection Security Level** drop-down to select the security level.

Step 3 In the **Expiration timeout for Rogue APs (seconds)** field, enter the timeout value.

Step 4 Select the **Validate Rogue Clients against AAA** check box to validate rogue clients against AAA server.

Step 5 Select the **Validate Rogue APs against AAA** check box to validate rogue access points against AAA server.

Step 6 In the **Rogue Polling Interval (seconds)** field, enter the interval to poll the AAA server for rogue information.

Step 7 Select the **Detect and Report Adhoc Networks** check box to enable detection of rogue adhoc networks.

Step 8 In the **Rogue Detection Client Number Threshold** field, enter the threshold to generate SNMP trap.

Step 9 In the **Auto Contain** section, enter the following details.

Step 10 Use the **Auto Containment Level** drop-down to select the level.

Step 11 Select the **Auto Containment only for Monitor Mode APs** check box to limit the auto-containment only to monitor mode APs.

Step 12 Select the **Rogue on Wire** check box to limit the auto-containment only to rogue APs on wire.

Step 13 Select the **Using our SSID** check box to limit the auto-containment only to rogue APs using one of the SSID configured on the controller.

Step 14 Select the **Adhoc Rogue AP** check box to limit the auto-containment only to adhoc rogue APs.

Step 15 Click **Apply**.

Configuring Rogue Policies (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**Example:**	Configures the rogue detection security level.

	Command or Action	Purpose
	`Device(config)# wireless wps rogue security-level custom`	You can select **critical** for highly sensitive deployments, **custom** for customizable security level, **high** for medium-scale deployments, and **low** for small-scale deployments.
Step 3	**wireless wps rogue ap timeout** *number of seconds* **Example:** `Device(config)# wireless wps rogue ap timeout 250`	Configures the expiration time for rogue entries, in seconds. Valid range for the time in seconds 240 seconds to 3600 seconds.
Step 4	**Example:** `Device(config)# wireless wps rogue client aaa`	Configures the use of AAA or local database to detect valid MAC addresses.
Step 5	**Example:** `Device(config)# wireless wps rogue client mse`	Configures the use of MSE to detect valid MAC addresses.
Step 6	**wireless wps rogue client notify-min-rssi** *RSSI threshold* **Example:** `Device(config)# wireless wps rogue client notify-min-rssi -128`	Configures the minimum RSSI notification threshold for rogue clients. Valid range for the RSSI threshold in dB is -128 - dB to -70 dB.
Step 7	**wireless wps rogue client notify-min-deviation** *RSSI threshold* **Example:** `Device(config)# wireless wps rogue client notify-min-deviation 4`	Configures the RSSI deviation notification threshold for rogue clients. Valid range for the RSSI threshold in dB is 0 dB to 10 dB.
Step 8	**wireless wps rogue ap aaa** **Example:** `Device(config)# wireless wps rogue ap aaa`	Configures the use of AAA or local database to classify rogue AP based on rogue AP MAC addresses.
Step 9	**wireless wps rogue ap aaa polling-interval** *AP AAA Interval* **Example:** `Device(config)# wireless wps rogue ap aaa polling-interval 120`	Configures rogue AP AAA validation interval. The valid range for the AP AAA interval in seconds is 60 seconds to 86400 seconds.
Step 10	**wireless wps rogue adhoc** **Example:** `Device(config)# wireless wps rogue adhoc`	Enables detecting and reporting adhoc rogue (IBSS).

	Command or Action	Purpose
Step 11	**wireless wps rogue client client-threshold** *threshold* **Example:** `Device(config)# wireless wps rogue client client-threshold 100`	Configures the rogue client per a rogue AP SNMP trap threshold. The valid range for the threshold is 0 to 256.
Step 12	**wireless wps rogue ap init-timer** **Example:** `Device(config)# wireless wps rogue ap init-timer 180`	Configures the init timer for rogue APs. The default timer value is set to 180 seconds. **Note** When a rogue AP is detected, an init timer is started and the rules are applied when this timer expires. This allows for rogue AP information to stabilize before applying any rules. However, you can change the value of this timer using this command. For instance, the init timer can be set to 0, if the rules need to be applied as soon as a new rogue AP is detected.

Rogue Detection Security Level

The rogue detection security level configuration allows you to set rogue detection parameters.

The available security levels are:

- Critical: Basic rogue detection for highly sensitive deployments.
- High: Basic rogue detection for medium-scale deployments.
- Low: Basic rogue detection for small-scale deployments.
- Custom: Default security-level, where all detection parameters are configurable.

Note When in Critical, High or Low, some rogue parameters are fixed and cannot be configured.

The following table shows parameter details for the three predefined levels:

Table 87: Rogue Detection: Predefined Levels

Parameter	Critical	High	Low
Cleanup Timer	3600	1200	240
AAA Validate Clients	Disabled	Disabled	Disabled

Parameter	Critical	High	Low
AAA Validate AP	Disabled	Disabled	Disabled
Adhoc Reporting	Enabled	Enabled	Enabled
Monitor-Mode Report Interval	10 seconds	30 seconds	60 seconds
Minimum RSSI	-128 dBm	-80 dBm	-80 dBm
Transient Interval	600 seconds	300 seconds	120 seconds
Auto Contain Works only on Monitor Mode APs.	Disabled	Disabled	Disabled
Auto Contain Level	1	1	1
Auto Contain Same-SSID	Disabled	Disabled	Disabled
Auto Contain Valid Clients on Rogue AP	Disabled	Disabled	Disabled
Auto Contain Adhoc	Disabled	Disabled	Disabled
Containment Auto-Rate	Enabled	Enabled	Enabled
Validate Clients with CMX	Enabled	Enabled	Enabled
Containment FlexConnect	Enabled	Enabled	Enabled

Setting Rogue Detection Security-level

Follow the procedure given below to set the rogue detection security-level:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless wps rogue security-level custom** **Example:** `Device(config)# wireless wps rogue security-level custom`	Configures rogue detection security level as custom.

	Command or Action	Purpose
Step 3	**wireless wps rogue security-level low** **Example:** `Device(config)# wireless wps rogue security-level low`	Configures rogue detection security level for basic rogue detection setup for small-scale deployments.
Step 4	**wireless wps rogue security-level high** **Example:** `Device(config)# wireless wps rogue security-level high`	Configures rogue detection security level for rogue detection setup for medium-scale deployments.
Step 5	**wireless wps rogue security-level critical** **Example:** `Device(config)# wireless wps rogue security-level critical`	Configures rogue detection security level for rogue detection setup for highly sensitive deployments.

Wireless Service Assurance Rogue Events

Wireless Service Assurance (WSA) rogue events, supported in Release 16.12.x and later releases, consist of telemetry notifications for a subset of SNMP traps. WSA rogue events replicate the same information that is part of the corresponding SNMP trap.

For all the exported events, the following details are provided to the wireless service assurance (WSA) infrastructure:

- MAC address of the rogue AP
- Details of the managed AP and the radio that detected the rogue AP with strongest RSSI
- Event-specific data such as SSID, channel for potential honeypot event, and MAC address of the impersonating AP for impersonation event

The WSA rogue events feature can scale up to four times the maximum number of supported APs and half of the maximum number of supported clients.

The WSA rogue events feature is supported on Cisco Catalyst Center and other third-party infrastructure.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**network-assurance enable** **Example:** `Device# network-assurance enable`	Enables wireless service assurance.

	Command or Action	Purpose
Step 3	**wireless wps rogue network-assurance enable** **Example:** `Device# wireless wps rogue network-assurance enable`	Enables wireless service assurance for rogue devices. This ensures that the WSA rogue events are sent to the event queue.

Monitoring Wireless Service Assurance Rogue Events

Procedure

- **show wireless wps rogue stats**

  Example:

```
Device# show wireless wps rogue stats

WSA Events
  Total WSA Events Triggered            : 9
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 2
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 3
    ROGUE_AP_IMPERSONATION_DETECTED     : 4
  Total WSA Events Enqueued             : 6
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 1
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 2
    ROGUE_AP_IMPERSONATION_DETECTED     : 3
```

  In this example, nine events have been triggered, but only six of them have been enqueued. This is because three events were triggered before the WSA rogue feature was enabled.

- **show wireless wps rogue stats internal**

  show wireless wps rogue ap detailed *rogue-ap-mac-addr*

  These commands show information related to WSA events into the event history.

Rogue Full Scale Quotas and Priorities

Feature History for Rogue Full Scale Quotas and Priorities

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 88: Feature History for Rogue Full Scale Quotas and Priorities

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	Rogue Full Scale Quotas and Priorities	The Rogue Full Scale Quotas and Priorities feature helps you to improve the scalability, performance, manageability, and serviceability of rogue Access Points (APs).

Rogue AP Scale Modes Per Class

The following are the modes that determine if a rogue AP is added to the database when it reaches maximum scale:

- **Quota**: Quotas are applied to each classification as a percentage of the maximum scale. This means that if a classification has quota X, then X percent of the rogue database is reserved for that classification. If the entire memory of the given classification is used up, the newly reported rogue APs under that classification are dropped.
- **Priority**: Priorities are applied to different classifications. When quotas are not configured, priority mode becomes the default mode.

  The priority for each classification is configured as follows:

  The default priority for malicious is **highest**. The default priority for custom is **high**. The default priority for unclassified is **medium**, and the default priority for friendly is **low**.

  Priorities are only applied when the maximum scale is reached. If a new rogue AP is classified and the maximum scale is reached, it is added to the database only if there are lower-priority rogue APs in the database. In such a case, the newest rogue AP entry of the lowest priority is deleted. Else, if there are no lower-priority rogue APs, the new rogue AP is dropped.
- **Hybrid**: Hybrid mode enables the use of quotas and priorities as a combination. Unused quota reserved for higher priority rogue APs are used by rogue APs of lower priority when space is available.

After reaching the maximum scale, if a new rogue AP is classified, the following logic is applied:

- If the number of stored rogue APs (in the class of the new rogue AP), is below the quota, store the new rogue AP. Delete the newest rogue AP of the classification with the lowest priority that is above the quota.
- Alternatively, check if there is a class with lower priority and is above the quota than the newly classified rogue AP. If such a class exists, delete the newest rogue AP of that lower-priority classification and store the new rogue AP.
- If none of the above conditions apply, drop the new rogue AP.

Table 89: Advantages and Disadvantages of Role-Scale Modes

Mode	Advantages	Disadvantages
Quota	Simple to use and understand.	• Memory is not used efficiently. • New rogue APs for a class that is already in its maximum quota are dropped. While the memory reserved for another class that does not have any rogue APs, stays empty. For example, this could lead to dropping malicious rogue APs, while there is still memory available.

Mode	Advantages	Disadvantages
Priority	• Simple to use and understand. • Utilizes the available memory. • Stores the important rogue APs.	Some of the lower-priority rogue AP classes might not be represented in the rogue database, if higher-priority rogue APs utilize all the available memory.
Hybrid	Utilizes the available memory, while providing quotas so that all the classes are represented in the database.	Difficult for users to understand the exact behavior.

Configuring Rogue AP Scale (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**[no] wireless wps rogue scale quota malicious** *percentage-malicious-rogue-AP* **custom** *percentage-custom-rogue-AP* **unclassified** *percentage-unclassified-rogue-AP* **friendly** *percentage-friendly-rogue-AP* **Example:** `Device(config)# wireless wps rogue scale quota malicious 5 custom 10 unclassified 3 friendly 5`	Configures rogue scale quota for malicious, custom, unclassified, and friendly rogue APs. The default value for quota is 0. The sum of all the quotas must be less than or equal to 100 percent. If the sum of all the configured quotas is equal to 0, then priority mode is used. If the sum of all the quotas is not equal to 0, then quota mode is used. If hybrid mode is configured, hybrid mode is used no matter what the quota configuration is. Hybrid mode with all the quotas equal to 0, is identical to the priority mode. **Note** Hybrid mode is enabled after the maximum scale is reached. All the rogue APs are stored before the maximum scale is reached.
Step 3	**[no] wireless wps rogue scale priority malicious** {**high** | **highest** | **low** | **medium**} **custom** {**high** | **highest** | **low** | **medium**} **unclassified** {**high** | **highest** | **low** | **medium**} **friendly** {**high** | **highest** | **low** | **medium**} **Example:**	Configures rogue scale priority for malicious, custom, unclassified, and friendly rogue APs. The default value for malicious is **highest**, the default value for custom is **high**, the default value for unclassified is **medium**, and the default value for friendly is **low**.

	Command or Action	Purpose
	`Device(config)# wireless wps rogue scale priority malicious highest custom high unclassified medium friendly low`	
Step 4	**[no] wireless wps rogue scale mode hybrid** **Example:** `Device(config)# wireless wps rogue scale mode hybrid`	Configures rogue scale hybrid mode. Unused quota reserved for higher-priority rogue APs are used by rogue APs of lower priority when space is available.

Verifying Rogue Scale Details

To verify the rogue scale details, run the following command:

```
Device# show wireless wps rogue stats
.
.
.
  Total Post Init/Max            : 0/4000
  Total/Max                      : 0/4200
  Init                           : 0
.
.
.
Classification
  Friendly                       : 0/0/0 (Total/Init/Quota[%])
  Malicious                      : 0/0/0 (Total/Init/Quota[%])
  Custom                         : 0/0/0 (Total/Init/Quota[%])
  Unclassified                   : 0/0/0 (Total/Init/Quota[%])
  Unknown                        : 0/0 (Total/Init)
.
.
.
Configured Quotas by Classification
  Custom         : <% of max scale>
  Friendly       : <% of max scale>
  Malicious      : <% of max scale>
  Unclassified   : <% of max scale>

Configured Priorities by Classification
  Custom          :  2 (High)
  Friendly        :  4 (Low)
  Malicious       :  1 (Highest)
  Unclassified    :  3 (Medium)

Configured Rogue Scale Mode: [Priority|Quota|Hybrid]
```

To view the rogue ad hoc summary, run the following command:

```
Device# show wireless wps rogue adhoc summary
Detect and report Ad-Hoc Networks : Enabled
Auto-Contain Ad-Hoc Networks      : Disabled
Total Number of Rogue Ad-Hoc      : 0
Friendly Ad-Hoc Rogues            : 0
Malicious Ad-Hoc Rogues           : 0
Custom Ad-Hoc Rogues              : 0
Unclassified Ad-Hoc Rogues        : 0
Unknown Ad-Hoc Rogues             : 0
Client MAC Address   Adhoc BSSID        Classification  State        # APs  Last Heard
```

CHAPTER 118

Classifying Rogue Access Points

- Information About Classifying Rogue Access Points, on page 1301
- Guidelines and Restrictions for Classifying Rogue Access Points, on page 1303
- How to Classify Rogue Access Points, on page 1303
- Monitoring Rogue Classification Rules, on page 1309
- Examples: Classifying Rogue Access Points, on page 1309

Information About Classifying Rogue Access Points

The controller software enables you to create rules that can organize and display rogue access points as Friendly, Malicious, Custom, or Unclassified.

By default, none of the classification rules are used. You need to enable them. Therefore, all unknown access points are categorized as Unclassified. When you create or change a rule, configure conditions, and enable it, all rogue access points are then reclassified. Whenever you change a rule, it is applied to all the access points (friendly, malicious, and unclassified).

Note

- Rule-based rogue classification does not apply to ad hoc rogues and rogue clients.
- You can configure up to 64 rogue classification rules per controller .

When the controller receives a rogue report from one of its managed access points, it responds as follows:

- If the unknown access point is in the friendly MAC address list, the controller classifies the access point as Friendly.
- If the unknown access point is not in the friendly MAC address list, the controller starts applying the rogue classification rules to the access point.
- If the rogue access point is manually classified, rogue rules are not applied to it.
- If the rogue access point matches the configured rules criteria, the controller classifies the rogue based on the classification type configured for that rule.
- If the rogue access point does not match any of the configured rules, the rogue remains unclassified.

  The controller repeats the previous steps for all the rogue access points.

- If the rogue access point is detected on the same wired network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if there are no configured rules. You can then manually contain the rogue to change the rogue state to Contained. If the rogue access point is not available on the network, the controller marks the rogue state as Alert. You can then manually contain the rogue.
- If desired, you can manually move the access point to a different classification type and rogue state.
- Before performing any classification, the rogue access points are temporarily marked as Pending.

Table 90: Classification Mapping

Rule-Based Classification Type	Rogue State
Custom	• Alert—No action is taken other than notifying the management station. The management station in the controller manages the controller and wired networks. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in Contained Pending state.
Delete	Deletes the rogue access point.
Friendly	• Internal—If the unknown access point poses no threat to WLAN security, you can manually configure it as Friendly, Internal. An example of this would be the access points in your lab network. • External—If the unknown access point is outside the network and poses no threat to WLAN security, you can manually configure it as Friendly, External. An example of this would be the access point in your neighboring coffee shop. • Alert—No action is taken other than notifying the management station. The management station manages the controller and wired networks.
Malicious	• Alert—No action is taken other than notifying the management station. The management station manages the controller and wired networks. • Threat—The unknown access point is found to be on the network and poses a threat to WLAN security. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in Contained Pending state.
Unclassified	• Alert— No action is taken other than notifying the management station. The management station manages the controller and wired networks. • Contained—The unknown access point is contained. If none of the managed access points are available for containment, the rogue is in contained pending state.

As mentioned earlier, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules. Alternatively, you can manually move the unknown access point to a different classification type and rogue state.

Guidelines and Restrictions for Classifying Rogue Access Points

- Classifying Custom type rogues is tied to rogue rules. Therefore, it is not possible to manually classify a rogue as Custom. Custom class change can occur only when rogue rules are used.
- Some SNMP traps are sent for containment by rule and every 30 minutes for rogue classification change.
- Rogue rules are applied on every incoming new rogue report in the controller in the order of their priority.
- After a rogue satisfies a rule and is classified, it does not move down the priority list for the same report.
- The rogue classification rules are re-evaluated at every report received by the managed access points. Hence, a rogue access point can move from one state to another, if a different rule matches the last report.
- If a rogue AP is classified as friendly or ignored, all rogue clients associated with it are not tracked.
- Until the controller discovers all the APs through neighbor reports from APs, the rogue APs are kept in unconfigured state for three minutes after they are detected. After 3 minutes, the rogue policy is applied on the rogue APs and the APs are moved to unclassified, friendly, malicious, or custom class. Rogue APs kept in unconfigured state means that no rogue policy has yet been applied on them.
- When a rogue BSSID is submitted for a containment on Cisco Catalyst 9800 Series Wireless Controller, if the controller has enough resources, it will contain. The APs that detect the particular contained rogue AP starts broadcasting the DEAUTH packets.

  Wireless client connected to the contained rogue BSSID will disconnect once DEAUTH packets are received. However, when the client assumes being in a connected state, repeatedly tries to reconnect and the wireless client's user browsing experience would be badly affected.

  Also, in a high RF environment like that of a stadium, though DEAUTH packets are broadcasted, client does not receive all of them because of RF disturbance. In this scenario, the client may not be fully disconnected but will be affected badly.
- The rouge AP manual classification limit has been enhanced from 625 to 10,000 configurations at a time. The rouge client manual classification limit has been enhanced from 625 to 10,000 configurations at a time.

How to Classify Rogue Access Points

Classifying Rogue Access Points and Clients Manually (GUI)

Procedure

Step 1 Choose **Monitoring > Wireless > Rogues**.

Step 2 In the **Unclassified** tab, select an AP to view the detail in the lower pane.

Step 3 Use the **Class Type** drop-down to set the status.

Step 4 Click **Apply**.

Classifying Rogue Access Points and Clients Manually (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue adhoc** {**alert** *mac-addr* | **auto-contain** | **contain** *mac-addr containment-level* | **internal** *mac-addr* | **external** *mac-addr*} **Example:** `Device(config)# wireless wps rogue adhoc alert 74a0.2f45.c520`	Detects and reports the ad hoc rogue. Enter one of these options after you enter the **adhoc** keyword: • **alert**—Sets the ad hoc rogue access point to alert mode. If you choose this option, enter the MAC address for the *mac-addr* parameter. • **auto-contain**—Sets the automatically containing ad hoc rogue to auto-contain mode. • **contain**—Sets the containing ad hoc rogue access point to contain mode. If you choose this option, enter the MAC address for the *mac-addr* parameter and containment level for the *containment-level* parameter. The valid range for *containment-level* is from 1 to 4. • **external**—Sets the ad hoc rogue access point as **external**. If you choose this option, enter the MAC address for the *mac-addr* parameter. • **internal**—Sets the ad hoc rogue access point as **internal**. If you choose this option, enter the MAC address for the *mac-addr* parameter.
Step 3	**wireless wps rogue ap** {**friendly** *mac-addr* **state** [**external** | **internal**] | **malicious** *mac-addr* **state** [**alert** | **contain** *containment-level*]} **Example:**	Configures the rogue access points. Enter one of the following options after the **ap** keyword:

	Command or Action	Purpose
	`Device(config)# wireless wps rogue ap malicious 74a0.2f45.c520 state contain 3`	• **friendly**—Configures the friendly rogue access points. If you choose this option, enter the MAC address for the *mac-addr* parameter. After that enter the **state** keyword followed by either of these options: **internal** or **external**. If you select an **internal** option, it indicates that you trust a foreign access point. If you select an **external** option, it indicates that you acknowledge the presence of a rogue access point. • **malicious**—Configures the malicious rogue access points. If you choose this option, enter the MAC address for the *mac-addr* parameter. After that enter the **state** keyword followed by either of these options: **alert** or **contain**. • **alert**—Sets the malicious rogue access point to **alert** mode. • **contain**—Sets the malicious rogue access point to **contain** mode. If you choose this option, enter the containment level for the *containment-level* parameter. The valid range is from 1 to 4.
Step 4	**wireless wps rogue client** {**contain** *mac-addr containment-level*} **Example:** `Device(config)# wireless wps rogue client contain 74a0.2f45.c520 2`	Configures the rogue clients. Enter the following option after you enter the **client** keyword: **contain**—Contains the rogue client. After you choose this option, enter the MAC address for the *mac-addr* parameter and the containment level for *containment-level* parameter. The valid range for *containment-level* is from 1 to 4.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Rogue Classification Rules (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies**.

Step 2 In the **Wireless Protection Policies** page, choose **Rogue AP Rules** tab.

Step 3 On the **Rogue AP Rules** page, click the name of the **Rule** or click **Add** to create a new one.

Step 4 In the **Add/Edit Rogue AP Rule** window that is displayed, enter the name of the rule in the **Rule Name** field.

Step 5 Choose the rule type from the following **Rule Type** drop-down list options:

- Friendly
- Malicious
- Unclassified
- Custom

Configuring Rogue Classification Rules (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps rogue rule** *rule-name* **priority** *priority* **Example:** `Device(config)# wireless wps rogue rule rule_3 priority 3`	Creates or enables a rule. While creating a rule, you must enter the priority for the rule. **Note** After creating a rule, you can edit the rule and change the priority only for the rogue rules that are disabled. You cannot change the priority for the rogue rules that are enabled. While editing, changing the priority for a rogue rule is optional.

Step 3	**classify** {**friendly state** {**alert** | **external** | **internal**} | **malicious state** {**alert** | **contained** }}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# classify friendly`
		Specifies the classification that needs to be applied to the rogue access points matching this rule.
		• **friendly**—Configures the friendly rogue access points. After that enter the **state** keyword followed by either of these options: **alert**, **internal**, or **external**. If you select an **internal** option, it indicates that you trust a foreign access point. If you select an **external** option, it indicates that you acknowledge the presence of a rogue access point.

	Command or Action	Purpose
		• **malicious**—Configures the malicious rogue access points. After that enter the state keyword followed by either of these options: alert or contained. • **alert**—Sets the malicious rogue access point to alert mode. • **contained**—Sets the malicious rogue access point to contained mode.

Step 4	**condition** {**client-count** *value* | **duration** *duration_value* | **encryption** | **infrastructure** | **rssi** | **ssid** *ssid_name* | **wildcard-ssid**}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# condition client-count 5`
		Adds the following conditions to a rule, which the rogue access point must meet:
		• **client-count**—Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, the access point could be classified as Malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point for the *value* parameter. The valid range is from 1 to 10 (inclusive), and the default value is 0.
		• **duration**—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period for the *duration_value* parameter. The valid range is from 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
		• **encryption**—Requires that the advertised WLAN does not have encryption enabled. You can choose **any** for any type of encryption, **off** for no encryption, **wpa1** for WPA encryption, **wpa2** for WPA2 encryption, **wpa3-owe** for WPA3 OWE encryption, or **wpa3-sae** for WPA3 SAE encryption.
		• **infrastructure**—Requires the SSID to be known to the controller.
		• **rssi**—Requires the rogue access point to be detected with a minimum RSSI value. If the classification is Friendly, the condition requires the rogue access point

	Command or Action	Purpose
		to be detected with a maximum RSSI value. The valid range is from –95 to –50 dBm (inclusive). • **ssid**—Requires the rogue access point to have a specific SSID. You could specify up to 25 different SSIDs. You should specify an SSID that is not managed by the controller. If you choose this option, enter the SSID for the *ssid_name* parameter. The SSID is added to the configured SSID list you just created. • **wildcard-ssid**—Allows you to specify an expression that could match an SSID string. You can specify up to 25 of these SSIDs.

Step 5	**match** {**all** | **any**}
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# match all`
		Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule for the rule to be matched and the rogue access point to adopt the classification type of the rule.

Step 6	**default**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# default`
		Sets a command to its default.

Step 7	**exit**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# exit`
	`Device(config)#`
		Exits the sub-mode.

Step 8	**shutdown**
	Example:
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# shutdown`
		Disables a particular rogue rule. In this example, the rule **rule_3** is disabled.

Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

	Command or Action	Purpose
Step 10	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 11	**wireless wps rogue rule shutdown** **Example:** `Device(config)# wireless wps rogue rule shutdown`	Disables all the rogue rules.
Step 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Rogue Classification Rules

You can monitor the rogue classification rules using the following commands:

Table 91: Commands for Monitoring Rogue Classification Rules

Command	Purpose
show wireless wps rogue rule detailed	Displays detailed information of a classification rule.
show wireless wps rogue rule summary	Displays a summary of the classification rules.

Examples: Classifying Rogue Access Points

This example shows how to classify a rogue AP with MAC address 00:11:22:33:44:55 as malicious and mark it for being contained by 2 managed APs:

```
Device# configure terminal
Device(config)# wireless wps rogue ap malicious 0011.2233.4455 state contain 2
```

This example shows how to create a rule that can categorize a rogue AP that is using SSID **my-friendly-ssid**, and it is seen for at least for 1000 seconds as friendly internal:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition ssid my-friendly-ssid
Device(config-rule)# condition duration 1000
Device(config-rule)# match all
Device(config-rule)# classify friendly state internal
Device(config-rule)# no shutdown
```

This example shows how to apply a condition that a rogue access point must meet:

```
Device# configure terminal
```

```
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition client-count 5
Device(config-rule)# condition duration 1000
Device(config-rule)# no shutdown
Device(config-rule)# end
```

This example shows a condition to classify rogue devices with the controller SSIDs as malicious:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)#  classify malicious state alert
Device(config-rule)#  condition duration 30
Device(config-rule)#  condition infrastructure ssid
Device(config-rule)#  match all
Device(config-rule)#  no shutdown
Device(config-rule)# end
```

CHAPTER 119

Advanced WIPS

- Feature History for Advanced WIPS, on page 1311
- Information About Advanced WIPS, on page 1312
- Enabling Advanced WIPS, on page 1315
- Syslog Support for Advanced WIPS, on page 1315
- Advanced WIPS Solution Components, on page 1316
- Supported Modes and Platforms, on page 1316
- Enabling Advanced WIPS(GUI), on page 1317
- Enabling Advanced WIPS (CLI), on page 1317
- Configuring Syslog Threshold for Advanced WIPS (CLI), on page 1318
- Viewing Advanced WIPS Alarms (GUI), on page 1318
- Verifying Advanced WIPS, on page 1319
- Verifying Syslog Configuration for Advanced WIPS, on page 1320

Feature History for Advanced WIPS

This table provides release and related information for the features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 92: Feature History for Advanced WIPS

Release	Feature Name	Feature Information
Cisco IOS XE Bengaluru 17.5.1	Advanced WIPS Signatures	Up to 15 additional signatures are supported.
Cisco IOS XE Bengaluru 17.6.1	Syslog Support for Advanced WIPs	From 17.6.1 release onwards: • Two additional signatures are supported. • Syslog support has been added to the controller for advanced WIPS.

Information About Advanced WIPS

The Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is a wireless intrusion threat detection and mitigation mechanism. The aWIPS uses an advanced approach to wireless threat detection and performance management. The AP detects threats and generates alarms. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention.

With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both wired and wireless networks and use that network intelligence to analyze attacks from multiple sources to accurately pinpoint and proactively prevent attacks, rather than wait until damage or exposure has occurred.

The following table shows the alarms introduced from Cisco IOS XE Bengaluru 17.5.1 onwards:

Table 93: Advanced WIPS Signatures and Definitions: From Cisco IOS XE Bengaluru 17.5.1 Onwards

Advanced WIPS Signature	Definition
RTS Virtual Carrier Sense Attack	This is an addition to the existing RTS Flood alarm introduced in Cisco IOS XE Bengaluru 17.4.x. The alarm is triggered when an RTS with a large duration is detected. An attacker can use these frames to exhaust air time and disrupt wireless client service.
CTS Virtual Carrier Sense Attack	This is an addition to the existing CTS Flood alarm introduced in Cisco IOS XE Bengaluru 17.4.x. The alarm is triggered when a CTS with large duration is detected. An attacker can use these frames to exhaust air time and disrupt wireless client service.
Deauthentication Flood by Pair	In the enhanced context of threat, both the source (attacker) and the destination (victim) of attacks (Track by Pair) have visibility.
Fuzzed Beacon	Fuzzed beacon is when invalid, unexpected, or random data is introduced into the beacon and replays those modified frames into the air. This causes unexpected behavior on the destination device, including driver crashes, operating system crashes, and stack-based overflows. This in turn allows the execution of the arbitrary code of the affected system.
Fuzzed Probe Request	Fuzzed probe request is when invalid, unexpected, or random data is introduced into a probe request and replays those modified frames into the air.
Fuzzed Probe Response	Fuzzed probe response is when invalid, unexpected, or random data is introduced into a probe response and replays those modified frames into the air.

Advanced WIPS Signature	Definition
PS Poll Flood by Signature	PS poll flood is when a potential hacker spoofs a MAC address of a wireless client and sends out a flood of PS poll frames. The AP sends out buffered data frames to the wireless client. This results in the client missing the data frames because it could be in the power safe mode.
Eapol Start V1 Flood by Signature	Extensible Authentication Protocol over LAN (EAPOL) start flood is when an attacker attempts to bring down the AP by flooding the AP with EAPOL-start frames to exhaust the AP's internal resources.
Reassociation Request Flood by Destination	Reassociation request flood is when a specific device tries to flood the AP with a large number of emulated and spoofed client reassociations to exhaust the AP's resources, particularly the client association table. When the client association table overflows, legitimate clients are not able to associate, causing a DoS attack.
Beacon Flood by Signature	Beacon flood is when stations actively search for a network that is bombarded with beacons from the networks that are generated using different MAC addresses and SSIDs. This flood prevents a valid client from detecting the beacons sent by corporate APs, which in turn initiates a DoS attack.
Probe Response Flood by Destination	Probe response flood is when a device tries to flood clients with a large number of spoofed probe responses from the AP. This prevents clients from detecting the valid probe responses sent by the corporate APs.
Block Ack Flood by Signature	Block ack flood is when an attacker transmits an invalid Add Block Acknowledgement (ADDBA) frame to the AP while spoofing the MAC address of the valid client. This process causes the AP to ignore any valid traffic transmitted from the client until it reaches the invalid frame range.
Airdrop Session	Airdrop session refers to the Apple feature called AirDrop. AirDrop is used to set up a peer-to-peer link for file sharing. This might create a security risk because of unauthorized peer-to-peer networks created dynamically in your WLAN environment.
Malformed Association Request	Malformed association request is when an attacker sends a malformed association request to trigger bugs in the AP. This results in a DoS attack.

Advanced WIPS Signature	Definition
Authentication Failure Flood by Signature	Authentication failure flood is when a specific device tries to flood the AP with invalid authentication requests spoofed from a valid client. This results in disconnection.
Invalid MAC OUI by Signature	Invalid MAC OUI is when a spoofed MAC address that does not have a valid OUI is used.
Malformed Authentication	Malformed authentication is when an attacker sends malformed authentication frames that can expose vulnerabilities in some drivers.

The following table shows the alarms introduced prior to Cisco IOS XE Bengaluru 17.5.1:

Table 94: Advanced WIPS Signatures: Prior Cisco IOS XE Bengaluru 17.5.1

Advanced WIPS Signatures
Authentication Flood Alarm
Association Flood Alarm
Broadcast Probe Flood Alarm
Disassociation Flood Alarm
Broadcast Dis-Association Flood Alarm
De-Authentication Flood Alarm
Broadcast De-Authentication Flood Alarm
EAPOL-Logoff Flood Alarm
CTS Flood Alarm
RTS Flood Alarm

Guidelines and Restrictions

- In the aWIPS profile, Cisco Aironet 1850 Series Access Points, Cisco Catalyst 9117 Series Access Points, and Cisco Catalyst 9130AX Series Access Points can detect EAPOL logoff attack and raise alarms accordingly, only on off-channel. They can not detect EAPOL logoff attack and raise alarms on on-channel.
- aWIPS profile download is not supported when Cisco Catalyst Center is configured using the fully qualified domain name (FQDN).

Enabling Advanced WIPS

From Cisco IOS XE Release 17.5.1 onwards, aWIPS security gets a higher priority over Hyperlocation/Fastlocate. The following are the possible scenarios.

All Catalyst APs supporting Fastlocate can be used together with aWIPS depending on the configuration and regardless of the AP mode.

In modes other than the Monitor mode for Cisco Aironet 4800 AP, if both aWIPS and Hyperlocation are enabled, only aWIPS is available.

Hyperlocation/Fastlocate	Advanced WIPS	Cisco Aironet 4800 AP Mode	Cisco Aironet 4800 AP Effective Feature
Enable	Enable	Any Non-Monitor	aWIPS[9]
Enable	Disable	Any Non-Monitor	Hyperlocation/Fastlocate
Disable	Disable	Any Non-Monitor	Hyperlocation/Fastlocate and aWIPS are disabled.
Disable	Enable	Any Non-Monitor	aWIPS
Enable	Enable	Monitor	aWIPS and Hyperlocation[10]
Disable	Enable	Monitor	aWIPS[11]
Enable	Disable	Monitor	Hyperlocation/Fastlocate
Disable	Disable	Monitor	Hyperlocation/Fastlocate and aWIPS are disabled.

[9] In modes other than the Monitor mode, if both aWIPS and Hyperlocation/Fastlocate are enabled, only aWIPS is available.

[10] In Monitor mode, if both aWIPS and Hyperlocation/Fastlocate are enabled, both aWIPS and Hyperlocation/Fastlocate are available.

[11] To monitor the status of aWIPS and Hyperlocation/Fastlocate simultaneously on AP, use the **show capwap client rcb** command.

Syslog Support for Advanced WIPS

This feature adds syslog support to the controller for Advanced WIPS.

The controller raises syslog messages when it receives alarms from an AP. The syslog messages go through throttling. If the same signature is detected from the same AP in a configured throttling interval, you must generate the syslog message for that alarm. For instance, if there were 100 occurrences of the same signature from the same AP within the throttling interval, say, 1 minute, you get to view only one syslog message in the controller in that 1-minute period instead of 100 messages.

Sample Syslog Format

The following is a sample syslog format:

```
Nov 18 20:45:23.746: %APMGR_AWIPS_SYSLOG-6-APMGR_AWIPS_MESSAGE: Chassis 1 R0/0: wncd: AWIPS
 alarm:(AP00B0.E19A.5720) 00b0.e19a.5720 Radio MAC 00b0.e19b.c300 detected Probe Response
Flood by Destination (10019)
```

The format covers the AP name, AP Ethernet MAC address, AP Radio MAC address, description (signature ID).

Note The syslog messages do not display any client information or context.

Advanced WIPS Solution Components

The aWIPS solution comprises the following components:

- Cisco Catalyst 9800 Series Wireless Controller
- Cisco Aironet Wave 2 APs
- Cisco Catalyst Center

Because the aWIPS functionality is integrated into Cisco Catalyst Center, the aWIPS can configure and monitor WIPS policies and alarms and report threats.

aWIPS supports the following capabilities:

- Static signatures

  From Cisco IOS XE, 17.4.1 onwards Cisco Catalyst Center can change threshold values and push new signature files to the AP.
- Enable or disable signature forensic capture from Cisco Catalyst Center.
- Standalone signature detection only
- Alarms only
- GUI support
- CLIs to view alarms
- Static signature file packaged with controller and AP image
- Export alarms to Cisco Catalyst Center through WSA channel

Note aWIPS alarm details such as the AP MAC address, alarm ID, alarm string, and signature ID are displayed on the Cisco Catalyst 9800 series wireless controller GUI.

Supported Modes and Platforms

aWIPS is supported on the following controllers:

- Cisco Catalyst 9800 Series Wireless Controllers
- Cisco Embedded Wireless Controller on Catalyst Access Points

Note aWIPS is not supported on Cisco IOS APs.

Enabling Advanced WIPS(GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.
Step 2 Click **Add**. The **Add AP Join Profile** window is displayed.
Step 3 In the **Add AP Join Profile** window, click the **Security** tab.
Step 4 Under the **aWIPS** section, check the **aWIPS Enable** check box.
Step 5 Click **Apply to Device**. You will go back the to **General** tab.
Step 6 Click the **Security** tab.
Step 7 Under the **aWIPS** section, check the **Forensic Enable** check box.
Step 8 Click **Apply to Device**.

Enabling Advanced WIPS (CLI)

To enable aWIPS from the controller and ensure that aWIPS has higher priority than Hyperlocation/Fastlocate, perform the following:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures the default AP profile.
Step 3	**awips** **Example:** `Device(config-ap-profile)# awips`	Enables aWIPS. **Note** aWIPS is disabled by default on the controller.

	Command or Action	Purpose
Step 4	**awips forensic** **Example:** `Device(conf-ap-profile)# awips forensic`	Enables forensics for aWIPS alarms.
Step 5	**hyperlocation** **Example:** `Device(config-ap-profile)# hyperlocation`	Enables Hyperlocation/Fastlocate on all the supported APs that are associated with this AP profile.
Step 6	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

Configuring Syslog Threshold for Advanced WIPS (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**awips-syslog throttle period** *syslog-throttle-interval* **Example:** `Device(config)# awips-syslog throttle period 38`	Configures the syslog threshold for aWIPS. *syslog-throttle-interval*: Enter the syslog throttle interval, in seconds. The range is from 30 to 600. **Note** The default throttling interval is 60 seconds.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Viewing Advanced WIPS Alarms (GUI)

Procedure

Step 1 Navigate to **Monitoring** > **Security** > **aWIPS**.

Step 2 To view the details of the alarms in the last 5 minutes, click the **Current Alarms** tab.

Step 3 To view the alarm count over an extended period of time, either hourly, for a day (24 hours) or more, click the **Historical Statistics** tab.

Step 4 Sort or filter the alarms based on the following parameters:

- **AP Radio MAC address**
- **Alarm ID**
- **Time Stamp**
- **Signature ID**
- **Alarm Description**
- **Alarm Message Index**

Verifying Advanced WIPS

To view the aWIPS status, use the **show awips status** *radio_mac* command:

```
Device# show awips status 0xx7.8xx8.2xx0

AP Radio MAC  AWIPS Status  Forensic Capture Status   Alarm Message Count
-------------------------------------------------------------------------------
0xx7.8xx8.2xx0      ENABLED       CONFIG_NOT_ENABLED  14691
```

The various aWIPS status indicators are:

- `ENABLED`: aWIPS enabled.
- `NOT_SUPPORTED`: The AP does not support AWIPS.
- `CONFIG_NOT ENABLED`: aWIPS is not enabled on the AP.

To view details of specific alarm signatures, use the **show awips alarm signature** *signature_id* command:

```
Device# show awips alarm signature 10001

AP Radio MAC    AlarmID   Timestamp          SignatureID    Alarm Description     Message
Index
-------------------------------------------------------------------------------------------------------------
0xx7.8xx8.2f80   1714    11/02/2020 13:02:19   10001       Authentication Flood     3966
```

To view alarm message statistics, use the **show awips alarm statistics** command:

```
Device# show awips alarm statistics
```

To view a list of alarms since the last clear, use the **show awips alarm ap** *ap_mac* **detailed** command:

```
Device# show awips alarm ap 0xx7.8xx8.2f80 detailed
AP Radio MAC    AlarmID     Timestamp              SignatureID   Alarm Description

-------------------------------------------------------------------------------------------------------------
0xx7.8xx8.2f80    2491    08/02/2022 17:44:40       10009         RTS Flood
```

To view detailed alarm information, use the **show awips alarm detailed** command:

```
Device# show awips alarm detailed
```

```
AP Radio MAC    AlarmID  Timestamp   SignatureID Alarm Description
-----------------------------------------------------------------------------------------------
7xx3.5xxd.d360  1        10/29/2020  23:21:27    10001 Authentication Flood by Source
dxxc.3xx5.9460  71       10/29/2020  23:21:27    10001 Authentication Flood by Source
7xx3.5xxd.d360  2        10/29/2020  23:21:28    10002 Association Request Flood by
Destination
dxxc.3xx5.9460  72       10/29/2020  23:21:28    10002 Association Request Flood by
Destination
```

To view the alarms on a specific AP, use the **show awips alarm ap** *radio_mac* **detailed** command:

Verifying Syslog Configuration for Advanced WIPS

To verify the syslog configuration for aWIPS, use the following command:

```
Device# show awips syslog throttle

Syslog Throttle Interval (seconds)

-----------------------------------------------------------------------------------------------

38
```

CHAPTER 120

Cisco TrustSec

- Information about Cisco TrustSec, on page 1321
- Cisco TrustSec Features, on page 1322
- Security Group Access Control List, on page 1323
- Inline Tagging, on page 1325
- Policy Enforcement, on page 1325
- SGACL Support for Wireless Guest Access, on page 1326
- Enabling SGACL on the AP (GUI), on page 1326
- Enabling SGACL on the AP, on page 1327
- Enabling SGACL Policy Enforcement Globally (CLI), on page 1328
- Enabling SGACL Policy Enforcement Per Interface (CLI), on page 1329
- Manually Configure a Device SGT (CLI), on page 1329
- Configuring SGACL, Inline Tagging, and SGT in Local Mode (GUI), on page 1330
- Configuring SGACL, Inline Tagging, and SGT in Local Mode, on page 1330
- Configuring ISE for TrustSec, on page 1331
- Verifying Cisco TrustSec Configuration, on page 1333

Information about Cisco TrustSec

Cisco TrustSec provides security improvements to Cisco network devices based on the capability to strongly identify users, hosts, and network devices within a network. TrustSec provides topology-independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

The key component of Cisco TrustSec is the Cisco Identity Services Engine (ISE). Cisco ISE can provision switches with TrustSec Identities and Security Group ACLs (SGACLs), though these may be configured manually on the switch.

Note You should manually clear the CTS environment data using the **clear cts environment-data** command before changing CTS server to a new one. This ensures that you get the updated data while running **show cts environment-data** command.

Cisco TrustSec Features

The table below lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

Cisco TrustSec Feature	Description
802.1AE Tagging (MACsec)	Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption. Between MACsec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices. This feature is only available between TrustSec hardware-capable devices.
Endpoint Admission Control (EAC)	EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).
Network Device Admission Control (NDAC)	NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
Security Group Access Control List (SGACL)	A Security Group Access Control List (SGACL) associates a Security Group Tag with a policy. The policy is enforced upon SGT-tagged traffic egressing the TrustSec domain.
Security Association Protocol (SAP)	After NDAC authentication, the Security Association Protocol (SAP) automatically negotiates keys and the cipher suite for subsequent MACSec link encryption between TrustSec peers. SAP is defined in IEEE 802.11i.
Security Group Tag (SGT)	An SGT is a 16-bit single label indicating the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet.

Cisco TrustSec Feature	Description
SGT Exchange Protocol (SXP)	Security Group Tag Exchange Protocol (SXP). With SXP, devices that are not TrustSec-hardware-capable can receive SGT attributes for authenticated users and devices from the Cisco Identity Services Engine (ISE) or the Cisco Secure Access Control System (ACS). The devices can then forward a sourceIP-to-SGT binding to a TrustSec-hardware-capable device will tag the source traffic for SGACL enforcement.

When both ends of a link support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a security association (SA).

Depending on your software version and licensing and link hardware support, SAP negotiation can use one of these modes of operation:

- Galois Counter Mode (GCM)—authentication and encryption
- GCM authentication (GMAC)— GCM authentication, no encryption
- No Encapsulation—no encapsulation (clear text)
- Null—encapsulation, no authentication or encryption

Security Group Access Control List

A security group is a group of users, end-point devices, and resources that share access control policies. Security groups are defined by the administrator in Cisco Identity Services Engine (ISE). As new users and devices are added to the Cisco TrustSec domain, the authentication server assigns these new entities to the appropriate security groups. Cisco TrustSec assigns each of the security group a unique 16-bit number whose scope is global in a Cisco TrustSec domain. The number of security groups in a wireless device is limited to the number of authenticated network entities. You do not have to manually configure the security group numbers.

After a device is authenticated, Cisco TrustSec tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT everywhere in the network, in the Cisco TrustSec header.

As the SGT contains the security group of the source, the tag can be referred to as the source SGT (S-SGT). The destination device is also assigned to a security group (destination SG) that can be referred to as the destination SGT (D-SGT), even though the Cisco TrustSec packet does not contain the security group number of the destination device.

You can control the operations that users can perform based on the security group assignments of users and destination resources, using the Security Group Access Control Lists (SGACLs). Policy enforcement in a Cisco TrustSec domain is represented by a permission matrix, with the source security group numbers on one axis and the destination security group numbers on the other axis. Each cell in the matrix body contains an ordered list of SGACLs, which specify the permissions that must be applied to packets originating from the source security group and destined for the destination security group. When a wireless client is authenticated, the controller downloads all the SGACLs in the matrix cells.

When a wireless client connects to the network, the client pushes all the ACLs to the controller .

Cisco TrustSec achieves role-based topology-independent access control in a network by assigning users and devices in the network to security groups and applying access control between the security groups. The SGACLs define access control policies based on the device identities. As long as the roles and permissions remain the same, changes to the network topology do not change the security policy. When a user is added to the wireless group, you simply assign the user to an appropriate security group; the user immediately receives permissions to that group.

The size of ACLs are reduced and their maintenance is simplified with the use of role-based permissions. With Cisco TrustSec, the number of Access Control Entities (ACEs) that are configured is determined by the number of permissions specified, resulting in a much smaller number of ACEs.

To know the list of Cisco APs that support SGACL, see the release notes: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html

Note Clients receive zero SGT value and DHCP clients receive an Automatic Private IP Addressing (APIPA) address when TrustSec policy “unknown to unknown” is denied in TrustSec matrix.

Clients receive correct SGT values and DHCP clients receive an IP address when TrustSec policy “unknown to unknown” is permitted in TrustSec matrix.

The scenarios supported for SGACLs on the Cisco Catalyst 9800 Series Wireless Controller are:

- Wireless-to-wireless (within Enterprise network):
  - Flex mode with local switching—SGACL enforcement is done on the egress AP when a packet leaves from a source wireless network to a destination wireless network.
  - Flex mode with central switching—SGACL enforcement is done on the egress AP. To achieve this, controller should export IP address to security group tag (IP-SGT) binding over SGT Exchange Protocol (SXP).
- Wired-to-wireless (DC-to-Enterprise network)—Enforcement takes place when a packet reaches the destination AP.
- Wireless-to-wired (Enterprise network-to-DC)—Enforcement takes place on the uplink switch when a packet reaches the ingress of the wired network.

Guidelines and Restrictions

- SGACL enforcement is carried out on the controller for local mode.
- SGACL enforcement is carried out on an AP for flex-mode APs performing local switching.
- SGACL enforcement for wireless clients is carried out either on the upstream switch or on the border gateway in a Branch-to-DC scenario.
- SGACL enforcement is not supported for non-IP or IP broadcast or multicast traffic.
- Per-WLAN SGT assignment is not supported.
- SGACL enforcement is not carried out for control-plane traffic between an AP and the wireless controller (for upstream or from upstream traffic).

- Non-static SGACL configurations are supported only for dynamic SGACL policies received from ISE.
- Static SGACL configuration on an AP is not supported.
- In case of Allow List model, you need to explicitly allow DHCP protocol for the client devices to get the DHCP IP address and then request the controller for SGACL policies.

Inline Tagging

Inline tagging is a transport mechanism using which a controller or AP understands the source SGT.

Transport mechanism is of two types:

- Central switching—For centrally switched packets, the controller performs inline tagging of all the packets sourced from wireless clients that are associated with the controller, by tagging it with the Cisco Meta Data (CMD) tag. For packets that are inbound from the distribution system, inline tagging also involves the controller stripping off the CMD header from the packet to learn the S-SGT tag. Thereafter, the controller forwards the packet including the S-SGT, for SGACL enforcement.
- Local switching—To transmit locally switched traffic, an AP performs inline tagging for packets that are associated with the AP and sourced from clients. To receive traffic, the AP handles both locally switched packets and centrally switched packets, uses the S-SGT tag for packets, and applies the SGACL policy.

With wireless Cisco TrustSec enabled on the controller , the choice of enabling and configuring SXP to exchange tags with the switches is optional. Both wireless Cisco TrustSec and SXP modes are supported; however, there is no use case to have both wireless Cisco TrustSec (on an AP) and SXP to be in the enabled state concurrently.

Consideration and Restriction for Inline Tagging over Port-Channel

- Configure the **cts manual** command on port-channel and its member interfaces to send or receive a tagged packet.
- If you downgrade to Cisco IOS XE releases that do not support inline tagging over port-channel, the port-channel may be suspended.

Note The inline tagging over port-channel is supported in Cisco IOS XE 17.3.517.6.317.8.1 release.

Policy Enforcement

Cisco TrustSec access control is implemented using ingress tagging and egress enforcement. At the ingress point to the Cisco TrustSec domain, the traffic from the source is tagged with an SGT containing the security group number of the source entity. The SGT is propagated across the domain with the traffic. At the egress point of the Cisco TrustSec domain, an egress device uses the source SGT (S-SGT) and the security group of the destination entity (D-SGT) to determine the access policy to apply from the SGACL policy matrix.

Policy enforcement can be applied to both central and local switched traffic on an AP. If wired clients communicate with wireless clients, the AP enforces the downstream traffic. If wireless clients communicate with wired clients, the AP enforces the upstream traffic. This way, the AP enforces traffic in both downstream and wireless-to-wireless traffic. You require S-SGT, D-SGT, and ACLs for the enforcement to work. APs get the SGT information for all the wireless clients from the information available on the Cisco ISE server.

Note A Cisco AP must be in either Listener or Both (Listener and Speaker) mode to enforce traffic because the Listener mode maintains the complete set of IP-SGT bindings. After you enable the enforcement on a an AP, the corresponding policies are downloaded and pushed to the AP.

SGACL Support for Wireless Guest Access

When a client joins the wireless network (WLAN), its session is managed by the Cisco Catalyst 9800 Series Wireless LAN Controller (WLC) that the AP is connected to is the foreign controller. Auto-Anchor Mobility allows a specific WLAN (for example, Guest WLAN) to be anchored to a particular controller, regardless of the client's entry point into the network. Auto-Anchor Mobility is the wireless Guest service where all guest traffic tunnels back to the DMZ controller irrespective of where they associate with the network.

In case of Auto-Anchor mobility, the following apply to Cisco TrustSec support:

- Classification: Occurs during authentication and hence on Foreign for Layer 2 security WLANs and on Anchor for Layer 3 security cases.
- Propagation: Always occurs at the Anchor where the client traffic enters the wired network.
- Enforcement: SGACL download and enforcement occurs on Anchor; the Anchor controller must have the connectivity to Cisco Identity Services Engine (ISE) and be registered as Network Access Server (NAS). Enforcement is not supported on foreign controller even when the enforcement CLI is configured on foreign controller.

This feature is supported in local mode and in Flex Central Switching of the controller. Flex mode with local switching and Fabric mode are not supported in guest scenarios as traffic does not go through the controller.

Roaming of a guest client occurs only at Guest Foreign controller and the Guest Anchor remains fixed. The different types of supported roam are Inter-Controller roaming and Intra-Controller roaming. Roaming under WebAuth pending is a special case which is also supported for Central Web Authentication (CWA) and Local Web Authentication (LWA).

Enabling SGACL on the AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, check **Inline Tagging** and **SGACL Enforcement** check boxes and choose the CTS Profile Name from the **CTS Profile Name** drop-down list.

Step 4 Click **Apply to Device**.

Enabling SGACL on the AP

Note Use the **no** form of the commands given below to disable the configuration. For example, **cts role-based enforcement** disables role-based access control enforcement for APs.

Before you begin

- Security Group Access Control List (SGACL) on an AP can be enabled only when the wireless controller is in FlexConnect mode.
- Configure the **cts manual** command on the uplink port to send or receive a tagged packet.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex xyz-flex-profile`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**cts role-based enforcement** **Example:** `Device(config-wireless-flex-profile)# cts role-based enforcement`	Enables role-based access control enforcement for the AP.
Step 4	**cts inline-tagging** **Example:** `Device(config-wireless-flex-profile)# cts inline-tagging`	Enables inline tagging on the AP.
Step 5	**cts profile** *profile-name* **Example:** `Device(config-wireless-flex-profile)# cts profile xyz-profile`	Enables the CTS profile name.
Step 6	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-wireless-flex-profile)# exit`	
Step 7	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site xyz-site`	Configures a site tag and enters site tag configuration mode.
Step 8	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile xyz-flex-profile`	Configures a flex profile.
Step 9	**exit** **Example:** `Device(config-site-tag)# exit`	Returns to global configuration mode.
Step 10	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures an AP and enters AP profile configuration mode.
Step 11	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag xyz-site`	Maps a site tag to an AP.

What to do next

Use the **show cts ap sgt-info** *ap-name*command to verify the SGACL configuration on the AP.

Enabling SGACL Policy Enforcement Globally (CLI)

You must enable SGACL policy enforcement globally on Cisco Catalyst 9800 Series Wireless Controller. The same configuration commands that are used for enforcement of IPv4 traffic apply for IPv6 traffic as well.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**cts role-based enforcement** **Example:**	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

	Command or Action	Purpose
	`Device(config)# cts role-based enforcement`	

Enabling SGACL Policy Enforcement Per Interface (CLI)

After enabling the SGACL policy enforcement globally, you will have to enable Cisco TrustSec-on the uplink interfaces.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface gigabitethernet** *interface number* **Example:** `Device(config)# interface gigabitethernet 1`	Specifies interface on which to enable or disable SGACL enforcement.
Step 3	**cts role-based enforcement** **Example:** `Device(config-if)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.
Step 4	**do show cts interface** **Example:** `Device(config-if)# do show cts interface`	Verifies that SGACL enforcement is enabled.

Manually Configure a Device SGT (CLI)

In normal Cisco TrustSec operation, the authentication server assigns an SGT to the device for packets originating from the device. You can manually configure an SGT to be used if the authentication server is not accessible, but an authentication server-assigned SGT will take precedence over a manually-assigned SGT.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**cts sgt** *sgt-value* **Example:** `Device(config-wireless-policy)# cts stg 200`	Specifies the Security Group Tag (SGT) number. Valid values are from 0 to 65,535.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.

Configuring SGACL, Inline Tagging, and SGT in Local Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name. The **Edit Policy Profile** is displayed.

Step 3 Choose **General** tab.

Step 4 In the **CTS Policy** settings, check or uncheck the **Inline Tagging** and **SGACL Enforcement** check boxes, and enter the **Default SGT** value.

Step 5 Click **Update & Apply to Device**.

Configuring SGACL, Inline Tagging, and SGT in Local Mode

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:**	Creates a policy profile for the WLAN.

	Command or Action	Purpose
	`Device(config)# wireless profile policy xyz-policy-profile`	
Step 3	**cts inline-tagging** **Example:** `Device(config-wireless-policy)# cts inline-tagging`	Enables CTS inline tagging. **Note** You will also need to configure the **cts manual** in the physical interface. If the **cts manual** is configured in the physical interface and **cts inline-tagging** is skipped, the packets will still remain tagged at egress in the controller.
Step 4	**cts role-based enforcement** **Example:** `Device(config-wireless-policy)# cts role-based enforcement`	Enables CTS SGACL enforcement.
Step 5	**cts sgt** *sgt-value* **Example:** `Device(config-wireless-policy)# cts sgt 100`	(Optional) Sets the default Security Group Tag (SGT). **Note** SGT is required for a user session only when the client uses open authentication, and not the ISE server.

Configuring ISE for TrustSec

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name.
Step 3	**address ipv4** *ip address* **Example:** `Device(config-radius-server)# address ipv4 124.3.50.62`	Specifies the primary RADIUS server parameters.

	Command or Action	Purpose
Step 4	**pac key** *key* **Example:** `Device(config-radius-server)# pac key cisco`	Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 5	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 6	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authc-server-group`	Creates a radius server-group identification. **Note** *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.
Step 7	**cts authorization list** *mlist-name* **Example:** `Device(config)# cts authorization list authc-list`	Creates a CTS authorization list.
Step 8	**aaa authorization network** *mlist-name* **group** *name* **Example:** `Device(config)# aaa authorization network default group group1`	Creates an authorization method list for web-based authorization. **Note** Ensure that the ISE IP address configured on your controller is the same as the IP address configured on ISE (**Work Center** > **TrustSec** > **Components** > **Trustsec AAA Servers**) **Note** If the ISE version is 002.005(000.239), 002.004(000.357), 002.003(000.298), 002.002(000.470), 002.001(000.474), 002.000(001.130), or 002.000(000.306), use the **access-session tls-version 1.0** command to download PAC from ISE. For other ISE versions, the above command is not required.

Verifying Cisco TrustSec Configuration

To display the wireless CTS SGACL configuration summary, use the following command:

```
Device# show wireless cts summary

Local Mode CTS Configuration

Policy Profile Name               SGACL Enforcement     Inline-Tagging   Default-Sgt
-------------------------------------------------------------------------------------
xyz-policy                        DISABLED              ENABLED          0
wireless-policy1                  DISABLED              DISABLED         0
w-policy-profile1                 DISABLED              DISABLED         0
default-policy-profile            DISABLED              DISABLED         0


Flex Mode CTS Configuration

Flex Profile Name                 SGACL Enforcement     Inline-Tagging
---------------------------------------------------------------------
xyz-flex                          DISABLED              ENABLED
demo-flex                         DISABLED              DISABLED
flex-demo                         DISABLED              DISABLED
xyz-flex-profile                  DISABLED              DISABLED
default-flex-profile              DISABLED              DISABLED
```

To display CTS-specific configuration status for various wireless profiles, use the following command:

```
Device# show cts wireless profile policy xyz-policy

Policy Profile Name           : xyz-policy
CTS
  Role-based enforcement         : ENABLED
  Inline-tagging                 : ENABLED
   Default SGT   : 100

Policy Profile Name            : foo2
CTS
  Role-based enforcement         : DISABLED
  Inline-tagging                 : ENABLED
  Default SGT           : NOT-DEFINED

Policy Profile Name                    : foo3
CTS
  Role-based enforcement         : DISABLED
  Inline-tagging                 : DISABLED
  Default SGT    : 65001
```

To display CTS configuration for a given wireless profile, use the following command:

```
Device# show wireless profile policy detailed xyz-policy

Policy Profile Name           : xyz-policy
Description                   :
Status                        : DISABLED
VLAN                          : 1
Client count                  : 0
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
!
```

```
.
.
.WGB Policy Params
  Broadcast Tagging           : DISABLED
  Client VLAN                 : DISABLED
Mobility Anchor List
  IP Address                                Priority
CTS
  Role-based enforcement         : ENABLED
  Inline-tagging                 : ENABLED
  Default SGT                   : NOT-DEFINED
```

CHAPTER 121

SGT Inline Tagging and SXPv4

- Introduction to SGT Inline Tagging on AP and SXPv4, on page 1335
- Creating an SXP Profile, on page 1335
- Configuring SGT Inline Tagging on Access Points, on page 1336
- Configuring an SXP Connection (GUI), on page 1336
- Configuring an SXP Connection, on page 1337
- Verifying SGT Push to Access Points, on page 1338

Introduction to SGT Inline Tagging on AP and SXPv4

The Cisco TrustSec (CTS) builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

The Scalable Group Tag (SGT) Exchange Protocol (SXP) is one of the several protocols that support CTS. CTS SXP version 4 (SXPv4) enhances the functionality of SXP by adding a loop detection mechanism to prevent stale binding in the network. In addition, Cisco TrustSec supports SGT inline tagging which allows propagation of SGT embedded in clear-text (unencrypted) ethernet packets.

When a wireless client is connected and is authenticated by ISE, the IP-SGT binding is generated on the controller . The same SGT is pushed to the AP along with the other client details.

For more details on SGT inline tagging on the AP and SXPv4, see the **Cisco TrustSec Configuration Guide** at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-3s/sec-usr-cts-xe-3s-book/sec-cts-sxpv4.html

Creating an SXP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless cts-sxp profile** *profile-name* **Example:** `Device(config)# wireless cts-sxp profile rr-profile`	Configures a wireless CTS profile and enters cts-sxp profile configuration mode.
Step 3	**cts sxp enable** **Example:** `Device(config-cts-sxp-profile)# cts sxp enable`	Enables SXP for Cisco TrustSec.

Configuring SGT Inline Tagging on Access Points

Follow the procedure given below to configure SGT inline tagging on APs:

Before you begin

- The SGTs pushed to the AP for inline tagging will only be from dynamic SGT allocation through ISE authentication. It is not supported for static bindings configured on the controller .
- SGTs will be pushed to an AP only when it is operating in flex mode.

To know the list of Cisco APs that support SGT inline tagging, see the release notes: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a wireless flex profile and enters the wireless flex profile configuration mode.
Step 3	**cts inline-tagging** **Example:** `Device(config-wireless-flex-profile)# cts inline-tagging`	Enables inline-tagging on the AP.

Configuring an SXP Connection (GUI)

Perform the following steps to set SXP global configuration.

Procedure

Step 1	In the **Global** section, select the **SXP Enabled** check box to enable SXP.
Step 2	Enter an IP address in the **Default Source IP** field.
Step 3	Enter a value in the **Reconciliation Period (sec)** field.
Step 4	Enter a value in the **Retry Period (sec)** field.
Step 5	Select the **Set New Default Password** check box. Selecting this check box displays the **Password Type** and **Enter Password** fields.
Step 6	Choose any one of the available types from the **Password Type** drop-down list.
Step 7	Enter a value in the **Enter Password** field.
Step 8	Click the **Apply** button.
Step 9	In the **Peer** section, click the **Add** button.
Step 10	Enter an IP address in the **Peer IP** field.
Step 11	Enter an IP address in the **Source IP** field.
Step 12	Choose any one of the available types from the **Password** drop-down list.
Step 13	Choose any one of the available types from the **Mode of Local Device** drop-down list.
Step 14	Click the **Save & Apply to Device** button.
Step 15	In the **AP** tab, click the **Add** button. The **Add SXP AP** dialog box appears.
Step 16	Enter a name for the profile in the **Profile Name** field.
Step 17	Set the **Status** field to **Enabled** to enable AP.
Step 18	Enter a value in the **Default Password** field.
Step 19	Enter a value (in seconds) for the **CTS Speaker Seconds, CTS Recon Period, CTS Retry Period, CTS Listener Maximum**, and **CTS Listener Minimum**
Step 20	In the **CTS SXP Profile Connections** section, click **Add**.
Step 21	Enter an IP address in the **Peer IP** field.
Step 22	Choose any one of the modes from the **Connection Mode** drop-down list. The available modes are **Both**, **Listener**, and **Speaker**.
Step 23	From the **Password Type** drop-down list, choose either **None** or **Default**.
Step 24	Click the **Add** button.
Step 25	Click the **Save & Apply to Device** button.

Configuring an SXP Connection

Follow the procedure given below to configure an SXP connection:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**cts sxp enable** **Example:** `Device(config)# cts sxp enable`	Enables CTS SXP support.
Step 3	**cts sxp connection peer** *ipv4-address* **password none mode local speaker** **Example:** `Device(config)# cts sxp connection peer 1.1.1.1 password none mode local speaker`	Configures the CTS-SXP peer address connection. **Note** The password need not be *none* always and the mode can either be Speaker or Listener, or Both.

What to do next

Use the following command to verify the configuration:

```
Device# show running-config | inc sxp
```

Verifying SGT Push to Access Points

When a wireless client is connected and authenticated by ISE, the IP-SGT binding is generated on the controller . This can be verified using the following commands:

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
1.1.1.1                 100     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

Use the following command to verify the SXP connections status:

```
Device# show cts sxp connections

 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP          : 40.1.1.1
Source IP        : 40.1.1.2
Conn status      : On
Conn version     : 4
```

```
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: none
Hold timer is running
Duration since last state change: 0:00:00:06 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

Use the following command to see the bindings learnt over SXP connection:

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
1.1.1.1                 100     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

Use the following commands on the AP to check the status of inline tagging on the AP and its IP-SGT bindings:

```
AP# show capwap client rcb

AdminState                          : ADMIN_ENABLED
OperationState                      : UP
Name                                : AP2C33.1185.C4D0
SwVer                               : 16.6.230.41
HwVer                               : 1.0.0.0
MwarApMgrIp                         : 9.3.72.38
MwarName                            : mohit-ewlc
MwarHwVer                           : 0.0.0.0
Location                            : default location
ApMode                              : FlexConnect
ApSubMode                           : Not Configured
CAPWAP Path MTU                     : 1485
CAPWAP UDP-Lite                     : Enabled
IP Prefer-mode                      : IPv4
AP Link DTLS Encryption             : OFF
AP TCP MSS Adjust                   : Disabled
LinkAuditing                        : disabled
Efficient Upgrade State             : Disabled
Flex Group Name                     : anrt-flex
AP Group Name                       : default-group
Cisco Trustsec Config
      AP Inline Tagging Mode                : Enabled
! The status can be Enabled or Disabled and is based on the tag that is pushed to the AP.
      AP Sgacl Enforcement                  : Disabled
      AP Override Status                    : Disabled

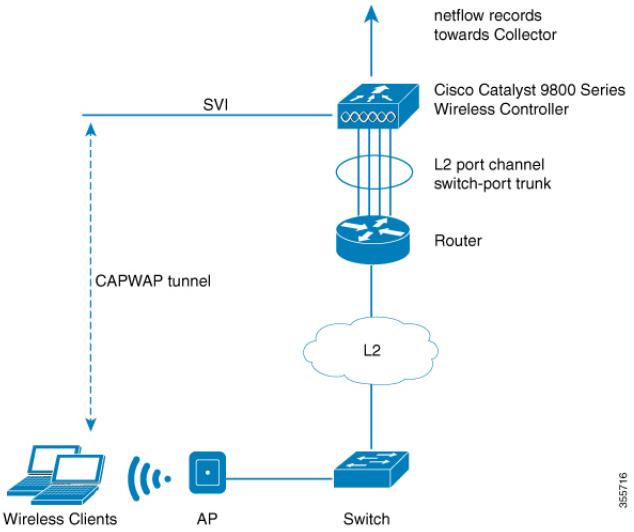

AP# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information
        IP SGT SOURCE
9.3.74.101  17  LOCAL
```

```
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of active   bindings = 1

Active IPv6-SGT Bindings Information
                      IP SGT SOURCE
fe80::c1d5:3da2:dc96:757d  17  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of active   bindings = 1
```

CHAPTER 122

Multiple Cipher Support

- Default Ciphersuites Supported for CAPWAP-DTLS, on page 1341
- Configuring Multiple Ciphersuites, on page 1342
- Setting Server Preference, on page 1343
- Verifying Operational Ciphersuites and Priority, on page 1343

Default Ciphersuites Supported for CAPWAP-DTLS

From Cisco IOS XE Bengaluru 17.5.1, Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)/Galois Counter Mode (GCM) ciphersuite with perfect forward secrecy (PFS) capability is added in the default list along with the existing AES128-SHA ciphersuite. All Cisco access point (AP) models, except the Cisco IOS APs, will prioritize this PFS ciphersuite for CAPWAP-DTLS under default configuration.

Note If link encryption is enabled for secure data channel traffic, then COS AP (DTLS client) will prioritize DHE-RSA-AES128-SHA over ECDHE/GCM ciphersuite.

During DTLS handshake, the preference order of the ciphersuites are important. This feature allows you to set the order of priority while configuring cipher suites.

When explicit ciphersuites are not configured, default ciphersuites that are listed in the table below are applied.

Table 95: Default Ciphersuites

Security Mode	Ciphersuite
FIPS and non-FIPS	• TLS_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Security Mode	Ciphersuite
WLANCC	• TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

This feature is supported on all variants of the Cisco Catalyst 9800 Series Wireless Controllers and APs, except Cisco Industrial Wireless 3702 Access Point.

For a list of controllers and APs supported in a particular release, see the release notes available at: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html

Configuring Multiple Ciphersuites

Note

- If a controller is loaded with a startup configuration having a version of ciphersuite selection configuration that is earlier than Cisco IOS XE Bengaluru 17.5.1, it it is auto converted to the latest version of ciphersuite selection configuration.
- Any change in the ciphersuite configuration results in AP flap.
- If you downgrade to a version earlier than Cisco IOS XE Bengaluru 17.5.1, ciphersuite configurations are lost.
- While downgrading to a version below 17.12.1 in FIPS mode or WLANCC mode, ensure ECDHE-RSA-AES128-GCM-SHA256 cipher suite is selected for AP DTLS (by default it is selected), else a downgrade will be impacted on all the COS APs.
- This can be verified by using the **show wireless certification config** command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dtls-ciphersuite priority** *priority-num ciphersuite* **Example:**	Sets priority for a particular cipher suite. Use zero (0) to set the highest priority.

	Command or Action	Purpose
	`Device(config)# ap dtls-ciphersuite priority 2 TLS_DHE_RSA_WITH_AES_128_CBC_SHA`	**Note** Configuration changes, if any, will automatically disconnect the existing APs.
Step 3	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Setting Server Preference

Ciphersuite configuration enforces the priority order in a DTLS handshake. To give equal priority for all the configured ciphersuites, then use **no ciphersuite server-preference** command in the corresponding AP join profile. By default, server preference is enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile xxy`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**[no] ciphersuite server-preference** **Example:** `Device(config-ap-profile)# [no] ciphersuite server-preference`	Sets the cipher suite server preference. Use the **no** form of this command to disable server preference. By default, server preference is enabled.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to global configuration mode.

Verifying Operational Ciphersuites and Priority

To view the operational ciphersuites and their priority, use the following command:

```
Device# show wireless certification config

WLANCC                          : Not Configured
AP DTLS Version                 : DTLS v1.0 - v1.2

AP DTLS Cipher Suite List:
```

```
  Priority                Ciphersuite
------------------------------------------------------------------------------
    0                     AES128-SHA
    1                     DHE-RSA-AES256-SHA256
```

CHAPTER 123

Configuring Secure Shell

- Information About Configuring Secure Shell , on page 1345
- Prerequisites for Configuring Secure Shell, on page 1347
- Restrictions for Configuring Secure Shell, on page 1348
- How to Configure SSH, on page 1349
- Monitoring the SSH Configuration and Status, on page 1351

Information About Configuring Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH and Device Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

SSH Servers, Integrated Clients, and Supported Versions

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

Note The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

SSH Configuration Guidelines

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If the SSH server is running on an active switch and the active switch fails, the new active switch uses the RSA key pair generated by the previous active switch.
- If you get CLI error messages after entering the **crypto key generate rsa** global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command.
- When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the **hostname** global configuration command.
- When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

Secure Copy Protocol Overview

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

For SSH to work, the switch needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

Note When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

Secure Copy Protocol

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying device configurations or switch image files. The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the device can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

SFTP Support

SFTP client support is introduced from Cisco IOS XE Gibraltar 16.10.1 release onwards. SFTP client is enabled by default and no separate configuration required.

The SFTP procedures can be invoked using the **copy** command, which is similar to that of **scp** and **tftp** commands. A typical file download procedure using **sftp** command can be carried out as shown below:

copy sftp://*user* :*password* @*server-ip*/*file-name* **flash0://** *file-name*

For more details on the **copy** command, see the following URL:
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/copy.html

Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the switch for secure shell (SSH):

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.
- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.
- SCP relies on SSH for security.
- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user must have appropriate authorization to use SCP.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the **copy** command. An authorized administrator can also do this from a workstation.
- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.)

- Configure a hostname and host domain for your device by using the **hostname** and **ip domain-name** commands in global configuration mode.

Note While upgrading from 16.11 to a later version, if you encounter a host key change by SSH client, you need to know the following:

- Wave 2 AP now supports a third key type ED25519 along with the RSA and ECDSA keys.
- The RSA and ECDSA keys are used for normal operations.
- The ED25519 key is used for FIPS mode.

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the device for secure shell.

- From Cisco IOS XE Dublin 17.10.x, Key Exchange and MAC algorithms like diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are not supported by default and it may impact some SSH clients that only support these algorithms. However, you can add them manually if required. For information on manually adding these algorithms, see the **SSH Algorithms for Common Criteria Certification** document available at: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html
- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- The device supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.
- The -l keyword and userid :{number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.
- To authenticate clients with FreeRADIUS over RADSEC, you should generate an RSA key longer than 1024 bit. Use the **crypto key generate rsa general-keys exportable label** *label-name* command to achieve this.

How to Configure SSH

Setting Up the Device to Run SSH

Follow the procedure given below to set up your device to run SSH:

Before you begin

Configure user authentication for local or remote access.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# Device# configure terminal`	Enters global configuration mode.
Step 2	**hostname** *hostname* **Example:** `Device(config)# hostname your_hostname`	Configures a hostname and IP domain name for your device. **Note** Follow this procedure only if you are configuring the device as an SSH server.
Step 3	**ip domain name** *domain_name* **Example:** `Device(config)# ip domain name your_domain`	Configures a host domain for your device.
Step 4	**crypto key generate rsa** **Example:** `Device(config)# crypto key generate rsa`	Enables the SSH server for local and remote authentication on the device and generates an RSA key pair. Generating an RSA key pair for the device automatically enables SSH. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use. **Note** Follow this procedure only if you are configuring the device as an SSH server.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config)# end`	Exits configuration mode.

Configuring the SSH Server

Follow the procedure given below to configure the SSH server:

Note This procedure is only required if you are configuring the device as an SSH server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip ssh version** [2] **Example:** `Device(config)# ip ssh version 2`	(Optional) Configures the device to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client.
Step 3	**ip ssh window-size** **Example:** Device(config)# **ip ssh window-size**	Specifies the SSH window size. The recommended window size is 32K or lesser that that. The default window size is 8912. Selecting **window-size** greater than 32K might have some impact on the CPU, until unless: • The network bandwidth is good. • Client can accommodate this size. • No latency in network. **Note** This CLI is recommended only for SCP operations and can be disabled once the copy is done.
Step 4	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*} **Example:** `Device(config)# ip ssh timeout 90`	Configures the SSH control parameters: • Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the

	Command or Action	Purpose
	`authentication-retries 2`	connection is established, the device uses the default time-out values of the CLI-based sessions. By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes. • Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5. Repeat this step when configuring both parameters.

Step 5	Use one or both of the following:
	• `line vty` *line_number* [*ending_line_number*]
	• **transport input ssh**
	Example:
	`Device(config)# line vty 1 10`
	or
	`Device(config-line)# transport input ssh`
		(Optional) Configures the virtual terminal line settings.
		• Enters line configuration mode to configure the virtual terminal line settings. For *line_number* and *ending_line_number*, specify a pair of lines. The range is 0 to 15.
		• Specifies that the device prevent non-SSH Telnet connections. This limits the router to only SSH connections.

Step 6	**end** **Example:** `Device(config-line)# end`	Returns to privileged EXEC mode.

Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

Table 96: Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.

Command	Purpose
show ssh	Shows the status of the SSH server.

CHAPTER 124

Encrypted Traffic Analytics

- Information About Encrypted Traffic Analytics, on page 1353
- Exporting Records to IPv4 Flow Export Destination, on page 1354
- Exporting Records to IPv6 Flow Export Destination, on page 1355
- Exporting Records to IPv4 and IPv6 Destination over IPFIX, on page 1355
- Allowed List of Traffic, on page 1356
- Configuring Source Interface for Record Export, on page 1357
- Configuring Source Interface for Record Export Without IPFIX, on page 1358
- Configuring ETA Flow Export Destination (GUI), on page 1359
- Enabling In-Active Timer, on page 1359
- Enabling ETA on WLAN Policy Profile, on page 1360
- Attaching Policy Profile to VLAN (GUI), on page 1361
- Attaching Policy Profile to VLAN, on page 1361
- Verifying ETA Configuration, on page 1362

Information About Encrypted Traffic Analytics

The Encrypted Traffic Analytics (ETA) leverages Flexible NetFlow (FNF) technology to export useful information about the flow to the collectors and gain visibility into the network.

Figure 39: Encrypted Traffic Analytics Deployed on Cisco Catalyst 9800 Series Wireless Controller in Local Mode



The wireless clients send data packets to the access point. The packets are then CAPWAP encapsulated and sent to the controller. This means that the actual client data is in the CAPWAP payload. To apply ETA on the client data, you need to strip the CAPWAP header before handing over the packet to the ETA module.

The ETA offers the following advantages:

- Enhanced telemetry based threat analytics.
- Analytics to identify malware.

Starting from Cisco IOS XE Amsterdam 17.1.1s, ETA inspection for IPv6 traffic is supported. ETA inspection for IPv6 traffic is enabled by default and no special configuration is required. This release also supports allowed list of IPv6 traffic, exporting ETA records to IPv4 or IPv6 export destination, exporting records over IPFIX (NetFlow v10), and configuring source interface for ETA exports. The records can be exported to IPv4 or IPv6 NetFlow collector.

Exporting Records to IPv4 Flow Export Destination

Follow the procedure given below to enable encrypted traffic analytics and configure a flow export destination:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Enables encrypted traffic analytics.

	Command or Action	Purpose
Step 3	**ip flow-export destination** *ip_address port_number* **Example:** `Device(config-et-analytics)# ip flow-export destination 120.0.0.1 2055`	Configures the NetFlow record export. Here, *port_number* ranges from 1 to 65535.
Step 4	**end** **Example:** `Device(config-et-analytics)# end`	Returns to privileged EXEC mode.

Exporting Records to IPv6 Flow Export Destination

Follow the procedure given below to enable encrypted traffic analytics and configure an IPv6 flow export destination.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Enables encrypted traffic analytics.
Step 3	**ipv6 flow-export destination** *ipv6-address port-number* **Example:** `Device(config-et-analytics)# ipv6 flow-export destination 2001:181:181::1 2055`	Specifies netflow record export destination IPv6 address and port. **Note** The maximum configurable limit for flow-export destinations is four (both IPv4 and IPv6 combined).
Step 4	**exit** **Example:** `Device(config-et-analytics)# exit`	Returns to global configuration mode.

Exporting Records to IPv4 and IPv6 Destination over IPFIX

This procedure provides efficient bandwidth utilization by allowing variable len fields for smaller data packets and also reduces the overall bandwidth requirements for transmission.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Enables encrypted traffic analytics.
Step 3	**ip flow-export destination** *ip-address port-number* **ipfix** **Example:** `Device(config-et-analytics)# ip flow-export destination 192.168.19.2 2055 ipfix`	Specifies NetFlow record export destination IP address, port and format.
Step 4	**ipv6 flow-export destination** *ipv6-address port-number* **ipfix** **Example:** `Device(config-et-analytics)# ipv6 flow-export destination 2001:181:181::1 2055 ipfix`	Specifies NetFlow record export destination IPv6 address, port and format. IPFIX allows you to collect flow information from network devices that support IPFIX protocol and analyze the traffic flow information by processing it through a netflow analyzer. **Note** Maximum configurable limit for flow-export destinations is four (both IPv4 and IPv6 combined).
Step 5	**exit** **Example:** `Device(config-et-analytics)# exit`	Returns to global configuration mode.

Allowed List of Traffic

You can add an allowed list of ACLs for both IPv4 and IPv6 traffic. Traffic from allowed list is skipped from ETA inspection and records are not generated for the matching traffic.

Before you begin

Configure an IPv4 or IPv6 access list.

- IPv4 ACL: **ip access-list standard** *acl_name*

  ```
  Device(config)# ip access-list standard eta-whitelist_ipv4
  ```

- IPv6 ACL: **ipv6 access-list** *acl_name*

  ```
  Device(config)# ipv6 access-list eta-whitelist_ipv6
  ```

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Enables encrypted traffic analytics.
Step 3	**whitelist acl** *acl-name* **Example:** `Device(config-et-analytics)# whitelist acl eta-whitelist`	Configures an allowed list for IPv4 or IPv6. **Note** You cannot add both IPv4 and IPv6 client traffic simultaneously to an allowed list, as a single ACL cannot have both IPv4 and IPv6 terms.
Step 4	**exit** **Example:** `Device(config-et-analytics)# exit`	Returns to global configuration mode.
Step 5	**sequence** *sequence-num* **permit udp any any eq tftp** **Example:** `Device(config-ipv6-acl)# sequence 10 permit udp any any eq tftp`	(Optional) Configures a sequence number and the access conditions to add any IPv6 TFTP traffic to allowed list.

Configuring Source Interface for Record Export

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Enables encrypted traffic analytics.
Step 3	**ip flow-export destination** *ip-address* **source-interface** *interface-name interface-number* **ipfix**	Specifies NetFlow record export destination IP address, source interface and format.

	Command or Action	Purpose
	Example: `Device(config-et-analytics)# ip flow-export destination 192.168.19.2 2055 source-interface loopback0 ipfix`	This allows the ETA export to use the IP address of the specified interface, as against using the IP address of the egress interface as the source address. The source interface is applicable for both IPv4 and IPv6 export destinations. **Note** Only one source interface can be specified and all exports use this source address.
Step 4	**ipv6 flow-export destination** *ipv6-address* **source-interface** *interface-nam interface-number* **ipfix** **Example:** `Device(config-et-analytics)# ipv6 flow-export destination 2001:181:181::1 2055 source-interface Vlan160 ipfix`	Specifies NetFlow record export destination IPv6 address, source interface and format.
Step 5	**exit** **Example:** `Device(config-et-analytics)# exit`	Returns to global configuration mode.

Configuring Source Interface for Record Export Without IPFIX

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Enables encrypted traffic analytics.
Step 3	**ip flow-export destination** *ip-address* **source-interface** *interface-name interface-number* **Example:** `Device(config-et-analytics)# ip flow-export destination 192.168.19.2 2055 source-interface loopback0 ipfix`	Specifies NetFlow record export destination IP address, source interface and format.

	Command or Action	Purpose
Step 4	**ipv6 flow-export destination** *ipv6-address* **source-interface** *interface-nam interface-number* **ipfix** **Example:** `Device(config-et-analytics)# ipv6 flow-export destination 2001:181:181::1 2055 source-interface Vlan160`	Specifies NetFlow record export destination IPv6 address, source interface and format.
Step 5	**exit** **Example:** `Device(config-et-analytics)# exit`	Returns to global configuration mode.

Configuring ETA Flow Export Destination (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **NetFlow**.

Step 2 Click the **Add** button. The **Create NetFlow** dialog box appears.

Step 3 Choose any one of the available templates from the **NetFlow Template** drop-down list.

Step 4 Enter an IPv4 or IPv6 address in the **Collector Address** field.

Step 5 From the **Whitelist ACL** drop-down list, choose the desired option.

Note To use this option, ensure that you select **Encrypted Traffic Analytics** from the **NetFlow Template** drop-down list.

Step 6 Enter a port number in the **Exporter Port** field. You must specify a value between 1 and 65535.

Step 7 Choose the desired option from the **Export Interface IP** drop-down list.

Step 8 Choose any one of the sampling methods from the **Sampling Method** drop-down list. The available options are **Deterministic**, **Random**, and **Full Netflow**.

Step 9 Enter a range for the sample. You must specify a value between 32 and 1032.

Step 10 Select the required interfaces/profile from the **Available** pane and move it to the **Selected** pane.

Step 11 Click the **Save & Apply to Device** button.

Enabling In-Active Timer

Follow the procedure given below to enable in-active timer:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**et-analytics** **Example:** `Device(config)# et-analytics`	Configures the encrypted traffic analytics.
Step 3	**inactive-timeout** *timeout-in-seconds* **Example:** `Device(config-et-analytics)# inactive-timeout 15`	Specifies the inactive flow timeout value. Here, *timeout-in-seconds* ranges from 1 to 604800.
Step 4	**end** **Example:** `Device(config-et-analytics)# end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Enabling ETA on WLAN Policy Profile

Follow the procedure given below to enable ETA on WLAN policy profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**et-analytics enable** **Example:** `Device(config-wireless-policy)# et-analytics enable`	Enables encrypted traffic analytics on the policy.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching Policy Profile to VLAN (GUI)

Perform the following steps to attach a policy profile to VLAN.

Procedure

Step 1 Check the **RADIUS Profiling** checkbox.

Step 2 From the **Local Subscriber Policy Name**, choose the required policy name.

Step 3 In the **WLAN Local Profiling** section, enable or disable the **Global State of Device Classification**, check the checkbox for **HTTP TLV Caching** and **DHCL TLV Caching**.

Step 4 In the **VLAN** section, choose the **VLAN/VLAN Group** from the drop-down list. Enter the Multicast VLAN.

Step 5 In the **WLAN ACL** section, choose the **IPv4 ACL** and **IPv6 ACL** from the drop-down list.

Step 6 In the **URL Filters** section, choose the **Pre Auth** and **Post Auth** from the drop-down list.

Step 7 Click **Save & Apply to Device**.

Attaching Policy Profile to VLAN

Follow the procedure given below to attach a policy profile to VLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan vlan-name`	Assigns the policy profile to the VLANs.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.

Verifying ETA Configuration

Verifying ETA Globally

To view the ETA global and interface details, use the following command:

```
Device# show platform software utd chassis active F0 et-analytics global

ET Analytics Global Configuration
ID: 1
All Interfaces: Off
IP address and port and vrf: 192.168.5.2:2055:0
```

To view the ETA global configuration, use the following command:

```
Device# show platform software et-analytics global

ET-Analytics Global state
=========================
 All Interfaces   : Off
 IP Flow-record Destination: 192.168.5.2 : 2055
 Inactive timer: 15
```

Note The **show platform software et-analytics global** command does not display the ETA enabled wireless client interfaces.

To view the ETA global state in datapath, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath runtime

ET-Analytics run-time information:

   Feature state: initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   WhiteList information :
       flag: False
       cgacl w0 :  n/a
       cgacl w1 :  n/a
   Flow CFG information  :
       instance ID       : 0x0
       feature ID        : 0x1
       feature object ID : 0x1
       chunk ID : 0xC
```

To view the ETA memory details, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath memory

ET-Analytics memory information:

   Size of FO            : 3200 bytes
   No. of FO allocs      : 0
   No. of FO frees       : 0
```

To view the ETA flow export in datapath, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats export

ET-Analytics 192.168.5.2:2055 vrf 0 Stats:
```

```
    Export statistics:
      Total records exported     : 5179231
      Total packets exported     : 3124873
      Total bytes exported       : 3783900196
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SPLT records exported:
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 309937
            responder->initiator : 329469
```

To view the ETA flow statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats flow

ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 0
      feature object frees  : 0
      flow create requests  : 0
      flow create matching  : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests          : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```

Verifying ETA on Wireless Client Interface

To view if a policy is configured with ETA, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : 160
Multicast VLAN                : 0
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : ENABLED
```

```
  Flex NAT PAT            : DISABLED
  Central Assoc               : ENABLED
```

To view the ETA status in the wireless client detail, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
<client_mac>

Wlclient Details for Client mac: 0026.c635.ebf8
  ---------------------------------
    Input VlanId  :  160
    Point of Presence      :  0
    Wlclient Input flags   :  9
    Instance ID   :  3
    ETA enabled   :  True
    client_mac_addr        :  0026.c635.ebf8

    bssid_mac_addr:  58ac.7843.037f
    Point of Attachment    :  65497
    Output vlanId :  160
    wlan_output_uidb       :  -1
    Wlclient Output flags  :  9
    Radio ID :  1
    cgacl w0 :  0x0
    cgacl w1 :  0x0
    IPv6 addr number       :  0
    IPv6 addr learning     :  0
```

To view clients in the ETA pending wireless client tree, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics
eta-pending-client-tree

CPP IF_H     DPIDX      MAC Address    VLAN  AS  MS WLAN          POA
------------------------------------------------------------------------------
   0X2A     0XA0000001  2c33.7a5b.827b  160   RN  LC xyz_ssid     0x90000003
   0X2B     0XA0000002  2c33.7a5b.80fb  160   RN  LC xyz_ssid     0x90000003
```

To view the QFP interface handle, use the following command:

```
Device#
show platform hardware chassis active qfp interface if-handle <qfp_interface_handle>

show platform hardware chassis active qfp interface if-handle 0X29
FIA handle - CP:0x27f3ce8  DP:0xd7142000
  LAYER2_IPV4_INPUT_ARL_SANITY
  WLCLIENT_INGRESS_IPV4_FWD
  IPV4_TVI_INPUT_FIA         >>> ETA FIA Enabled
  SWPORT_VLAN_BRIDGING
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x27f3d30  DP:0xd7141780
  IPV4_VFR_REFRAG (M)
  IPV4_TVI_OUTPUT_FIA        >>> ETA FIA Enabled
  WLCLIENT_EGRESS_IPV4_FWD
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
```

Note The *qfp_interface_handle* ranges from 1 to 4294967295.

To view the ETA pending wireless client tree statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics statistics

Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 2
Counter                                          Value
-----------------------------------------------------------------
Enable ETA on wireless client called             0
Delete ETA on wireless client called             0
ETA global cfg init cb TVI FIA enable error      0
ETA global cfg init cb output SB read error      0
ETA global cfg init cb output SB write error     0
ETA global cfg init cb input SB read error       0
ETA global cfg init cb input SB write error      0
ETA global cfg init cb TVI FIA enable success    0
ETA global cfg uninit cb ingress feat disable    0
ETA global cfg uninit cb ingress cfg delete e    0
ETA global cfg uninit cb egress feat disable     0
ETA global cfg uninit cb egress cfg delete er    0
ETA pending list insert entry called             4
ETA pending list insert invalid arg error        0
ETA pending list insert entry exists error       0
ETA pending list insert no memory error          0
ETA pending list insert entry failed             0
ETA pending list insert entry success            4
ETA pending list delete entry called             2
ETA pending list delete invalid arg error        0
ETA pending list delete entry missing            0
ETA pending list delete entry remove error       0
ETA pending list delete entry success            2
```

To view the allowed list configuration, use the following commands:

```
Device# show platform software et-analytics global

ET-Analytics Global state
=========================
 All Interfaces   : Off
 IP Flow-record Destination: 192.168.5.2 : 2055
 Inactive timer: 15
 whitelist acl eta-whitelist

Device# show platform hardware chassis active qfp feature et-analytics datapath runtime
ET-Analytics run-time information:
 Feature state: initialized (0x00000004)
 Inactive timeout      : 15 secs (default 15 secs)
   WhiteList information :
       flag: True
       cgacl w0 :  0xd9ae9c80
       cgacl w1 :  0x20000000
   Flow CFG information  :
       instance ID       : 0x0
       feature ID        : 0x0
       feature object ID : 0x0
       chunk ID : 0x4
```

To view the ETA export statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats export

ET-Analytics Stats:
    Export statistics:
      Total records exported     : 5179231
      Total packets exported     : 3124873
      Total bytes exported       : 3783900196
```

```
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SPLT records exported:
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 309937
            responder->initiator : 329469
```

To view the ETA flow statistics, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats flow

ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 0
      feature object frees  : 0
      flow create requests  : 0
      flow create matching  : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests          : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```

To view the ETA datapath runtime detail, use the following command:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath runtime

ET-Analytics run-time information:
   Feature state         : initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   WhiteList information :
       flag              : True
       cgacl w0          :  0xd9ae1e10
       cgacl w1          :  0x20000000
   Flow CFG information  :
       instance ID       : 0x0
       feature ID        : 0x0
       feature object ID : 0x0
       chunk ID          : 0x4
```

CHAPTER 125

FIPS

- FIPS, on page 1367
- Guidelines and Restrictions for FIPS, on page 1368
- FIPS Self-Tests, on page 1368
- Configuring FIPS, on page 1369
- Configuring FIPS in HA Setup, on page 1370
- Verifying FIPS Configuration, on page 1371

FIPS

Federal Information Processing Standard (FIPS) 140-2 is a security standard used to validate cryptographic modules. The cryptographic modules are produced by the private sector for use by the U.S. government and other regulated industries (such as financial and healthcare institutions) that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information.

Note Cisco TrustSec (CTS) is not supported when the controller is in FIPS mode.

For more information about FIPS, see

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html.

With FIPS in enabled state, some passwords and pre-shared keys must have the following minimum lengths:

- For Software-Defined Access Wireless, between the controller and map server, a pre-shared key (for example, the LISP authentication key) is used in authentication of all TCP messages between them. This pre-shared key must be at least 14 characters long.
- The ISAKMP key (for example, the Crypto ISAKMP key) must be at least 14 characters long.

Limitations for FIPS

- The console of APs get disabled when the controller is operating in FIPS mode.
- The weak or legacy cipher like SHA1 is not supported in FIPS mode.
- APs would not reload immediately, if you change the FIPS status.

Note We recommend a minimum RSA key size of 2048 bits under RADSEC when operating in FIPS mode. Otherwise, the RADSEC fails.

Guidelines and Restrictions for FIPS

- In the controller switches, a legacy key is used to support the legacy APs. However, in FIPS mode, the crypto engine detects the legacy key as a weak key and rejects it by showing the following error message: "**% Error in generating keys: could not generate test signature.**" We recommend that you ignore such error messages that are displayed during the bootup of the controller (when operating in FIPS mode).
- SSH clients using SHA1 will not be able to access the controller when you enable FIPS.

Note You need to use FIPS compliant SSH clients to access the controller.

- While configuring WLAN ensure that the PSK length must be minimum of 15 characters. If not, the APs will not be able to join the controller after changing tags..
- TrustSec is not supported.
- PAC key configuration is not supported.
- FIPS is not compatible with level-6 encrypted passwords. Additionally, 802.1X authentications will fail if the RADIUS shared secret uses a type-6 encryption key.

FIPS Self-Tests

A cryptographic module must perform power-up self-tests and conditional self-tests to ensure that it is functional.

Power-up self-tests run automatically after the device powers up. A device goes into FIPS mode only after all self-tests are successfully completed. If any self-test fails, the device logs a system message and moves into an error state. Also, if the power-up self test fails, the device fails to boot.

Using a known-answer test (KAT), a cryptographic algorithm is run on data for which the correct output is already known, and then the calculated output is compared to the previously generated output. If the calculated output does not equal the known answer, the known-answer test fails.

Power-up self-tests include the following:

- Software integrity
- Algorithm tests

Conditional self-tests must be run when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

The device uses a cryptographic algorithm known-answer test (KAT) to test FIPS mode for each FIPS 140-2-approved cryptographic function (encryption, decryption, authentication, and random number generation) implemented on the device. The device applies the algorithm to data for which the correct output is already known. It then compares the calculated output to the previously generated output. If the calculated output does not equal the known answer, the KAT fails.

Conditional self-tests run automatically when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

Conditional self-tests include the following:

- Pair-wise consistency test—This test is run when a public or private key-pair is generated.
- Continuous random number generator test—This test is run when a random number is generated.
- Bypass
- Software load

Configuring FIPS

Ensure that both the active and standby controllers have the same FIPS authorization key.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**fips authorization-key** *key* **Example:** `Device(config)# fips authorization-key 12345678901234567890123456789012`	Enables the FIPS mode. The key length should be of 32 hexadecimal characters. **Note** When FIPS is enabled, you may need to trigger more than one factory reset using the reset button. To disable FIPS mode on the device, use the **no** form of this command.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

What to do next

You must reboot the controller whenever you enable or disable the FIPS mode.

Configuring FIPS in HA Setup

While bringing up HA pair in FIPS mode, you need to configure both active and standby controllers with the same FIPS authorization key independently before forming HA pair.

If you configure FIPS authorization key after forming HA pair, the FIPS authorization key configuration will not be synced with the standby. Rebooting HA pair at this state causes reload loop. To avoid this, you need to perform the following:

- Break the HA pair.
- Configure the same FIPS authorization key independently on both the members.
- Pair up members.

To configure FIPS in HA setup, perform the following:

1. Power off both the members of the stack.
2. Power on only member1, and wait for the controller to come up and prompt for login from the console.
3. Login successfully with your valid credentials, and execute the following commands:

```
Show fips status
Show fips authorization-key
Show romvar
Show chassis
```

Note Keep the configured FIPS authorization key handy.

4. Configure the FIPS key, if you have not configured one earlier.

```
conf t
fips authorization-key <32 hex char>
```

5. Save and power off the member1.
6. Power on only member2 and wait for the controller to come up and prompt for login from the console.
7. Login successfully with your valid credentials, and execute the following commands:

```
Show fips status
Show fips authorization-key
Show romvar
Show chassis
```

Note Keep the configured FIPS authorization key handy.

8. Configure the FIPS key, if you have not configured one earlier.

Note The key value must be the same in both the members of the stack.

```
conf t
fips authorization-key <32 hex char>
```

9. Save and power off the member2.
10. Power on both the members together, and wait for the stack to form.
11. Monitor any crash or unexpected reload.

Note It is expected that members must not reload due to FIPS issue.

Verifying FIPS Configuration

You can verify FIPS configuration using the following commands:

Use the following **show** command to display the installed authorization key:

```
Device# show fips authorization-key
FIPS: Stored key (16) : 12345678901234567890123456789012
```

Use the following **show** command to display the status of FIPS on the device:

```
Device# show fips status
Chassis is running in fips mode
```

CHAPTER 126

Internet Protocol Security

- Information about Internet Protocol Security, on page 1373
- Internet Key Exchange Version 1 Transform Sets, on page 1374
- Configure IPSec Using Internet Key Exchange Version 1, on page 1375
- Internet Key Exchange Version 2 Transform Sets, on page 1377
- Configure IPSec Using Internet Key Exchange Version 2, on page 1378
- IPsec Transforms and Lifetimes, on page 1380
- Use of X.509 With Internet Key Exchange Version, on page 1381
- IPsec Session Interruption and Recovery, on page 1382
- Example: Configure IPSec Using ISAKMP, on page 1383
- Verifying IPSec Traffic, on page 1383
- Example: Configure IPSec Using Internet Key Exchange Version 2, on page 1384
- Verifying IPSec With Internet Key Exchange Version 2 Traffic , on page 1385

Information about Internet Protocol Security

Internet Protocol Security (IPsec) is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPsec ensures confidentiality, integrity, and authenticity of data communications across a public network. IPsec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

Cisco Catalyst 9800 Series Wireless Controller supports IPsec configuration. The support for IPSec secures syslog traffic.

This section provides information about how to configure IPsec between Cisco Catalyst 9800 Series Wireless Controller and syslog (peer IP).

IPsec provides the following network security services:

- Data confidentiality: The IPsec sender can encrypt packets before transmitting them across a network.
- Data integrity: The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- Data origin authentication: The IPsec receiver can authenticate the source of the sent IPsec packets. This service is dependent upon the data integrity service.
- Anti-replay: The IPsec receiver can detect and reject replayed packets.

IPsec provides secure *tunnels* between two peers, such as two devices. The administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these *tunnels* are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol.

With IPsec, administrators can define the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. (The access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.)

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the device attempts to match the packet to the access list specified in that entry.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as cisco, connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the device. *Applicable* packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Access lists associated with IPsec crypto map entries also represent the traffic that the device needs protected by IPsec. Inbound traffic is processed against crypto map entries--if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Internet Key Exchange Version 1 Transform Sets

An Internet Key Exchange version 1 (IKEv1) transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

Privileged administrators can specify multiple transform sets and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows specified by that crypto map entry's access list.

During IPsec security association negotiations with IKE, peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of both peers' IPsec SAs.

Note If a transform set definition is changed during operation that the change is not applied to existing security associations, but is used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

The following snippet helps to configure IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with *encryption aes 256*:

```
device # conf t
device (config)#crypto isakmp policy 1
device (config-isakmp)# hash sha
device (config-isakmp)# encryption aes
```

Configure IPSec Using Internet Key Exchange Version 1

Follow the procedure given below to configure IPsec IKEv1 to use AES-CBC-128 for payload encryption:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto isakmp policy** *priority* **Example:** `Device(config)# crypto isakmp policy 1`	Defines an Internet Key Exchange (IKE) policy and assigns a priority to the policy. • *priority*: Uniquely identifies the IKE policy and assigns a priority to the policy. Valid values: 1 to 10,000; 1 is the highest priority.
Step 3	**hash sha** **Example:** `Device(config-isakmp)# hash sha`	Specifies the hash algorithm.
Step 4	**encryption aes** **Example:** `Device(config-isakmp)# encryption aes`	Configures IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with ‘encryption aes 256’.

	Command or Action	Purpose
		Note The authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in section IPsec Transforms and Lifetimes. If AES 128 is selected here, then the highest keysize that can be selected on the device for ESP is AES 128 (either CBC or GCM). Both confidentiality and integrity are configured with the **hash sha** and **encryption aes** commands respectively. As a result, confidentiality-only mode is disabled.
Step 5	**authentication pre-share** **Example:** `Device(config-isakmp)# authentication pre-share`	Configures IPsec to use the specified preshared keys as the authentication method. Preshared keys require that you separately configure these preshared keys.
Step 6	**exit** **Example:** `Device(config-isakmp)# exit`	Exits config-isakmp configuration mode.
Step 7	**crypto isakmp key** *keystring* **address** *peer-address* **Example:** `Device(config)# crypto isakmp key cisco123!cisco123!CISC address 192.0.2.1`	Configures a preshared authentication key. **Note** To ensure a secure configuration, we recommend that you enter the pre-shared keys with at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). The device supports pre-shared keys up to 127 characters in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.
Step 8	**group 14** **Example:** `Device(config-isakmp)# group 14`	Specifies the Diffie-Hellman (DH) group identifier as 2048-bit DH group 14 and selects DH Group 14 (2048-bit MODP) for IKE. However, 19 (256-bit Random ECP), 24

	Command or Action	Purpose
		(2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP) are also allowed and supported.
Step 9	**lifetime** *seconds* **Example:** `Device(config-isakmp)# lifetime 86400`	Specifies the lifetime of the IKE SA. The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values. • *seconds*: Time, in seconds, before each SA expires. Valid values: 60 to 86,400; default value: 86,400. **Note** The shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec SAs can be set up more quickly.
Step 10	**crypto isakmp aggressive-mode disable** **Example:** `Device(config-isakmp)# crypto isakmp aggressive-mode disable`	Ensures all IKEv1 Phase 1 exchanges will be handled in the default main mode.
Step 11	**exit** **Example:** `Device(config-isakmp)# exit`	Exits config-isakmp configuration mode.

Internet Key Exchange Version 2 Transform Sets

An Internet Key Exchange Version 2 (IKEv2) proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation. The following snippet helps in configuring the IPsec with IKEv2 functionality for the device:

```
device # conf t
device(config)#crypto ikev2 proposal sample
device(config-ikev2-proposal)# integrity sha1
device (config-ikev2-proposal)# encryption aes-cbc-128
device(config-ikev2-proposal)# group 14
device(config-ikev2-proposal)# exit
device(config)# crypto ikev2 keyring keyring-1
device (config-ikev2-keyring)# peer peer1
device (config-ikev2-keyring-peer)# address 192.0.2.4 255.255.255.0
```

```
device (config-ikev2-keyring-peer)# pre-shared-key cisco123!cisco123!CISC
device (config-ikev2-keyring-peer)# exit
device(config)#crypto ikev2 keyring keyring-1
device (config-ikev2-keyring)# peer peer1
device (config-ikev2-keyring-peer)# address 192.0.2.4 255.255.255.0
device (config-ikev2-keyring-peer)# pre-shared-key cisco123!cisco123!CISC
device (config-ikev2-keyring-peer)# exit
device(config)#crypto logging ikev2
```

Configure IPSec Using Internet Key Exchange Version 2

Follow the procedure given below to configure the IPsec with IKEv2:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto ikev2 proposal** *name* **Example:** `Device(config)# crypto ikev2 proposal name`	Defines an IKEv2 proposal name.
Step 3	**integrity sha1** **Example:** `Device(config-ikev2-proposal)# integrity sha1`	Defines an IKEv2 proposal name.
Step 4	**encryption aes-cbc-128** **Example:** `Device(config-ikev2-proposal)# encryption aes-cbc-128`	Configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with encryption aes-cbc-256. AES-GCM-128 and AES-GCM-256 can also be selected similarly.

	Command or Action	Purpose
		Note The authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in section IPsec Transforms and Lifetimes. If AES 128 is selected here, then the highest keysize that can be selected on the device for ESP is AES 128 (either CBC or GCM). Both confidentiality and integrity are configured with the **hash sha** and **encryption aes** commands respectively. As a result, confidentiality-only mode is disabled.
Step 5	**group 14** **Example:** `Device(config-ikev2-proposal)# group 14`	Selects DH Group 14 (2048-bit MODP) for IKE. However, 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP) are also allowed and supported.
Step 6	**exit** **Example:** `Device(config-ikev2-proposal)# exit`	Exists IKEv2 proposal configuration mode.
Step 7	**crypto ikev2 keyring** *keyring-name* **Example:** `Device(config)# crypto ikev2 keyring keyring-1`	Defines an IKEv2 keyring.
Step 8	**peer** *peer-name* **Example:** `Device(config-ikev2-keyring)# peer peer1`	Defines the peer or peer group.
Step 9	**address {ipv4-address [mask] | ipv6-address prefix}** **Example:** `Device(config-ikev2-keyring)# address 192.0.2.4 255.255.255.0`	Specifies an IPv4 or IPv6 address or range for the peer. **Note** This IP address is the IKE endpoint address and is independent of the identity address.
Step 10	**pre-shared-key** *local* **Example:**	Specifies the preshared key for the peer. You can enter the local or remote keyword to

	Command or Action	Purpose
	`Device(config-ikev2-keyring)# pre-shared-key cisco123!cisco123!CISC`	specify an asymmetric preshared key. By default, the preshared key is symmetric. **Note** To ensure a secure configuration, we recommend that you enter the pre-shared keys with at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). The device supports pre-shared keys up to 127 characters in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time. HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: *pre-shared-key hex [hex key]*. For example: pre-shared-key hex 0x6A6B6C. This configures IPsec to use pre-shared keys.
Step 11	**exit** **Example:** `Device(config-ikev2-keyring)# exit`	Exits IKEv2 keyring peer configuration mode.
Step 12	**crypto logging ikev2** **Example:** `Device(config)# crypto logging ikev2`	Enables IKEv2 syslog messages. **Note** The configuration above is not a complete IKE v2 configuration, and that additional settings will be needed.

IPsec Transforms and Lifetimes

Regardless of the IKE version selected, the device must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.

`device (config)#` **`crypto ipsec transform-set example esp-aes 128 esp-sha-hmac`**

Note that this configures IPsec ESP to use HMAC-SHA-1 and AES-CBC-128. To change this to the other allowed algorithms the following options can replace **esp-aes 128** in the command above:

Encryption Algorithm	Command
AES-CBC-256	**esp-aes 256**
AES-GCM-128	**esp-gcm 128**
AES-GCM-256	**esp-gcm 256**

Note The size of the key selected here must be less than or equal to the key size selected for the IKE encryption setting. If AES-CBC-128 was selected there for use with IKE encryption, then only AES-CBC-128 or AES-GCM-128 may be selected here.

```
device(config-crypto)# mode tunnel
```

This configures tunnel mode for IPsec. Tunnel is the default, but by explicitly specifying tunnel mode, the device will request tunnel mode and will accept only tunnel mode.

```
device(config-crypto)# mode transport
```

This configures transport mode for IPsec.

```
device(config)# crypto ipsec security-association lifetime seconds 28800
```

The default time value for Phase 2 SAs is 1 hour. There is no configuration required for this setting since the default is acceptable. However to change the setting to 8 hours as claimed in the Security Target the crypto ipsec security-association lifetime command can be used as specified above.

```
device(config)# crypto ipsec security-association lifetime kilobytes 100000
```

This configures a lifetime of 100 MB of traffic for Phase 2 SAs. The default amount for this setting is 2560KB, which is the minimum configurable value for this command. The maximum configurable value for this command is 4GB.

Use of X.509 With Internet Key Exchange Version

Cisco Catalyst 9800 Series Wireless Controller supports RSA and ECDSA based certificates.

Once X.509v3 keys are installed on the device, they can be set for use with IKEv1 with the commands:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto isakmp** *policy-name* **Example:** `Device(config)#crypto isakmp policy 1`	Defines an Internet Key Exchange (IKE) policy and assigns a priority to the policy.

	Command or Action	Purpose
Step 3	**authentication [remote | local] rsa-sig** **Example:** `Device(config-isakmp)#authentication rsa-sig`	Uses RSA based certificates for IKEv1 authentication.
Step 4	**authentication [remote | local] ecdsa-sig** **Example:** `Device(config-isakmp)#authentication ecdsa-sig`	Uses ecdsa based certificates for IKEv1 authentication.

For IKEv2 Commands

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto ikev2 profile sample** **Example:** `Device(config)# crypto ikev2 profile sample`	Defines an Internet Key Exchange (IKE) policy and assigns a profile.
Step 3	**authentication [remote | local] rsa-sig** **Example:** `Device(config-ikev2-profile)# authentication rsa-sig`	Uses RSA based certificates for IKEv1 authentication.
Step 4	**authentication [remote | local] ecdsa-sig** **Example:** `Device(config-ikev2-profile)# authentication ecdsa-sig`	Uses ecdsa based certificates for IKEv1 authentication. Authentication fails if an invalid certificate is loaded.

IPsec Session Interruption and Recovery

If an IPsec session with a peer is unexpectedly interrupted, the connection will be broken. In this scenario, no administrative interaction is required. The IPsec session will be reestablished (a new SA set up) once the peer is back online.

Example: Configure IPSec Using ISAKMP

The following sample outputs display the IPSec **isakmp** configuration:

```
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 28800

crypto isakmp key 0 Cisco!123 address 192.0.2.4
crypto isakmp peer address 192.0.2.4

crypto ipsec transform-set aes-gcm-256 esp-gcm 256
 mode tunnel

crypto map IPSEC_ewlc_to_syslog 1 ipsec-isakmp
 set peer 192.0.2.4
 set transform-set aes-gcm-256
 match address acl_ewlc_to_syslog

interface Vlan15
 crypto map IPSEC_ewlc_to_syslog
end
```

Verifying IPSec Traffic

The following example shows how to verify the IPSec traffic configuration in isakmp configuration:

```
Device# show crypto map
Crypto Map IPv4 "IPSEC_ewlc_to_syslog" 1 ipsec-isakmp
        Peer = 192.0.2.4
        Extended IP access list acl_ewlc_to_syslog
            access-list acl_ewlc_to_syslog permit ip host 192.0.2.2 host 192.0.2.4
        Current peer: 192.0.2.4
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                aes-gcm-256:  { esp-gcm 256  } ,
        }
        Interfaces using crypto map IPSEC_ewlc_to_syslog:
                Vlan15

Device# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.5       192.0.2.4       QM_IDLE           1011 ACTIVE

IPv6 Crypto ISAKMP SA

Device# show crypto ipsec sa

interface: Vlan15
    Crypto map tag: IPSEC_ewlc_to_syslog, local addr 192.0.2.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.5/255.255.255.255/0/0)
```

```
   remote ident (addr/mask/prot/port): (192.0.2.4/255.255.255.255/0/0)
   current_peer 192.0.2.4 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1626, #pkts encrypt: 1626, #pkts digest: 1626
    #pkts decaps: 1625, #pkts decrypt: 1625, #pkts verify: 1625
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.0.2.5, remote crypto endpt.: 192.0.2.4
     plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Vlan15
     current outbound spi: 0x17FF2F4C(402599756)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x4B77AD78(1266134392)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2041, flow_id: HW:41, sibling_flags FFFFFFFF80004048, crypto map:
IPSEC_ewlc_to_syslog
        sa timing: remaining key lifetime (k/sec): (4607904/1933)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x17FF2F4C(402599756)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2042, flow_id: HW:42, sibling_flags FFFFFFFF80004048, crypto map:
IPSEC_ewlc_to_syslog
        sa timing: remaining key lifetime (k/sec): (4607904/1933)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:

Device# show ip access-lists acl_ewlc_to_syslog
Extended IP access list acl_ewlc_to_syslog
    10 permit ip host 192.0.2.5 host 192.0.2.4 (17 matches)
```

Example: Configure IPSec Using Internet Key Exchange Version 2

The following sample outputs display the IPSec **IKEv2** configuration:

```
topology : [192.0.2.6]DUT — (infra) — PEER[192.0.2.9]

ikev2 config in 192.0.2.6 (peer is 192.0.2.9)
hostname for 192.0.2.9: Edison-M1
hostname for 192.0.2.6: prsna-nyquist-192.0.2.6

ip access-list extended ikev2acl
 permit ip host 192.0.2.6 host 192.0.2.9
```

```
crypto ikev2 proposal PH1PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy PH1POLICY
 proposal PH1PROPOSAL

crypto ikev2 keyring PH1KEY
  peer Edison-M1
  address 192.0.2.9
  pre-shared-key Cisco!123Cisco!123Cisco!123


crypto ikev2 profile PH1PROFILE
 match identity remote address 192.0.2.9 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local PH1KEY

crypto ipsec transform-set aes256-sha1 esp-aes 256 esp-sha-hmac
 mode tunnel

crypto map ikev2-cryptomap 1 ipsec-isakmp
 set peer 192.0.2.9
 set transform-set aes256-sha1
 set ikev2-profile PH1PROFILE
 match address ikev2acl

interface Vlan15
 ip address 192.0.2.6 255.255.255.0
 crypto map ikev2-cryptomap
```

Verifying IPSec With Internet Key Exchange Version 2 Traffic

The following example shows how to verify the IPSec traffic configuration in IKEv2 configuration:

```
Device# show ip access-lists
Extended IP access list ikev2acl
    10 permit ip host 192.0.2.6 host 192.0.2.9 (80 matches)

prsna-nyquist-192.0.2.6#show crypto map
Crypto Map IPv4 "ikev2-cryptomap" 1 ipsec-isakmp
        Peer = 192.0.2.9
        IKEv2 Profile: PH1PROFILE
        Extended IP access list ikev2acl
            access-list ikev2acl permit ip host 192.0.2.6 host 192.0.2.9
        Current peer: 192.0.2.9
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                aes256-sha1:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map ikev2-cryptomap:
                Vlan15
Device# show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
```

```
1         192.0.2.6/500         192.0.2.9/500          none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK,
Auth verify: PSK
      Life/Active Time: 86400/1002 sec
      CE id: 1089, Session-id: 2
      Status Description: Negotiation done
      Local spi: 271D20169FE91074       Remote spi: 13895472E3B910AF
      Local id: 192.0.2.6
      Remote id: 192.0.2.9
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: disabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
Device# show crypto ipsec sa detail

interface: Vlan15
    Crypto map tag: ikev2-cryptomap, local addr 192.0.2.6

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.6/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.0.2.9/255.255.255.255/0/0)
   current_peer 192.0.2.9 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 80, #pkts encrypt:80, #pkts digest: 80
    #pkts decaps: 80, #pkts decrypt: 80, #pkts verify: 80
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
    #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
    #pkts invalid prot (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
    ##pkts replay failed (rcv): 0
    #pkts tagged (send): 0, #pkts untagged (rcv): 0
    #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (recv) 0

     local crypto endpt.: 192.0.2.6, remote crypto endpt.: 192.0.2.9
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Vlan15
     current outbound spi: 0xB546157A(3041269114)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x350925BC(889791932)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 838, flow_id: 838, sibling_flags FFFFFFFF80000040, crypto map:
ikev2-cryptomap
        sa timing: remaining key lifetime (k/sec): (4287660676/2560)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:
```

```
     outbound esp sas:
      spi: 0xB546157A(3041269114)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 837, flow_id: 837, sibling_flags FFFFFFFF80000040, crypto map:
ikev2-cryptomap
        sa timing: remaining key lifetime (k/sec): (4287660672/2560)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

CHAPTER 127

Transport Layer Security Tunnel Support

- Information About Transport Layer Security Tunnel Support, on page 1389
- Configuring a Transport Layer Security Tunnel, on page 1390
- Verifying a Transport Layer Security Tunnel, on page 1391

Information About Transport Layer Security Tunnel Support

The Cisco Catalyst 9800 Series Wireless Controller requires direct access to a public cloud to implement the teleworker solution using Cisco OfficeExtend Access Points (OEAPs). With the introduction of Transport Layer Security (TLS) tunnel support from Cisco IOS XE Amsterdam 17.3.2 onwards, the controller can now reach a public cloud automatically. This helps Cisco Catalyst Center on Cloud to establish TLS communication channels with the controller to perform monitor and manage of wireless solutions.

The TLS connection ensures that the configuration and telemetry are reliably and securely communicated between the controller and the Digital Network Architecture (DNA) on Cloud. The TLS tunnel encrypts all the data that is sent over the TCP connection. The TLS tunnel provides a more secure protocol across the internet. After the controller discovery, the Cisco Catalyst Center on Cloud uses Cisco DNA Assurance and Automation features to manage the controller centrally.

Cisco Plug and Play

The Cisco Plug and Play solution is a converged solution that provides a highly secure, scalable, seamless, and unified zero-touch deployment experience.

Plug-n-Play Agent

The Cisco Plug and Play (PnP) agent is an embedded software component that is present in all the Cisco network devices that support simplified deployment architecture. The PnP agent understands and interacts only with a PnP server. The PnP agent, using DHCP, DNS, or other such methods, tries to acquire the IP address of the PnP server with which it wants to communicate. After a server is found and a connection is established, the agent communicates with the PnP server to perform deployment-related activities.

For more information on Cisco Plug and Play, see the Cisco Plug and Play Feature Guide.

The Transport Layer Security Tunnel (TLS) over PnP feature is supported on the following controllers:

- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-L Wireless Controller

Configuring a Transport Layer Security Tunnel

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**crypto tls-tunnel** *TLS-tunnel-name* **Example:** `Device(config)# crypto tls-tunnel cloud-primary`	Configures a crypto TLS tunnel channel.
Step 3	**server {ipv4** <*A.B.C.D*> | **ipv6** <*X.X.X.X::X*> | **url** <*url-name*>} **port 443** <*1025-65535*> **Example:** `Device(config-crypto-tls-tunnel)# server ipv4 172.31.255.255 port 4043`	Specifies the server IPv4 address, IPv6 address, or URL name and the port number.
Step 4	**overlay interface** *interface-name interface-num* **Example:** `Device(config-crypto-tls-tunnel)# overlay interface Loopback0`	Specifies the overlay interface and interface number. An overlay interface is a logical, multiaccess, multicast-capable interface. An overlay interface encapsulates Layer 2 frames in IP unicast or multicast headers.
Step 5	**local interface** *interface-name interface-num* **priority** rank **Example:** `Device(config-crypto-tls-tunnel)# local-interface vlan 1 priority 1`	Specifies the LAN interface type, number, and the priority rank. **Note** Currently, the tunnel supports only one WAN interface with priority 1 and does not support the list of WAN interfaces with multiple priorities.
Step 6	**psk id** *identity* **key** *options* **Example:** `Device(config-crypto-tls-tunnel)# psk id test key`	Specifies a preshared key and password options.
Step 7	**pki trustpoint trustpoint trustpoint-label [sign | verify]** **Example:** `Device(config-crypto-tls-tunnel)# pki trustpoint tsp1 sign`	Specifies the trustpoints for use with the RSA signature authentication method as follows: • **sign**: Use the certificate from the trustpoint which is sent to the peer.

	Command or Action	Purpose
		• **verify**: Use the certificate from the trustpoint to verify the certificate received from the peer. **Note** • If the **sign** or **verify** keyword is not specified, the trustpoint is used for signing and verification. • In TLS Tunnel block, authentication can be done using either pre-shared key (PSK) or PKI (certificate based).
Step 8	(Optional) **cc-mode** **Example:** `Device(config-crypto-tls-tunnel)# cc-mode`	Indicates a common criteria mode, which is a Federal Information Processing Standards (FIPS) mode.
Step 9	**no shutdown** **Example:** `Device(config-crypto-tls-tunnel)# no shutdown`	Enables the TLS tunnel.
Step 10	**end** **Example:** `Device(config-crypto-tls-tunnel)# end`	Returns to privileged EXEC mode.

Verifying a Transport Layer Security Tunnel

The TLS client support includes BinOS processes using Linux Tun/Tap Interface. To verify the TLS client summary details, use the following command:

```
Device# show platform software tlsc client summary
TLS Client - Config Summary

Name         ID     Gateway    Port   Auth     Trustpoint  DPD Time    Rekey Time  Retry
Time
-------------------------------------------------------------------------------------------
fqdn         0                 8443   PSK      N/A            60          300         20
```

To verify the TLS client session detail, session statistics, tunnel statistics, and DNS counters, use the following command:

```
Device# show platform software client detail <tls-name>

Session Name     : fqdn
FQDN resolved IP : 10.255.255.255
```

```
ID              : 0
Created         : 04/20/21 00:36:42
Updated         : 04/22/21 05:56:03
State           : Up (Rekey)
Up Time         : 04/21/21 20:30:21 (9 hours 25 minutes 45 seconds)
Down Time       : 04/21/21 20:30:01
Rekey Time      : 04/22/21 05:55:51 (15 seconds)

TLS Session Statistics
Up Notifications    : 3
Down Notifications  : 2
Rekey Notifications : 636
DP State Updates    : 0
DPD Cleanups        : 0

Packets From         Packets To    Packet Errors To     Bytes From           Bytes To
-------------------------------------------------------------------------------------
BinOS                 80             0                    0                    0
IOSd                   0             0                    0                    0

TLS Client             0             0                    0                    0


TLS Tunnel Statistics

Type       Tx Packets           Rx Packets
----------------------------------------
Total        0                    80
CSTP Ctrl   3836                 3836
CSTP Data    80                   0

Type       Requests             Responses
--------------------------------------
CSTP Cfg   639                  639
CSTP DPD   3197                 3197

Invalid CSTP Rx         : 0
Injected Packet Success : 0
Injected Packet Failed  : 0
Consumed Packets        : 0

TLS Tunnel DNS Counters

DNS Resolve Request Success Count : 641
DNS Resolve Request Failure Count : 0
DNS Resolve Success Count         : 639
DNS Resolve Failure Count         : 2
```

To verify the TLS client global statistics, use the following command.

```
Device# show platform software tlsc statistics
TLS Client: Global Statistics

Session Statistics
Up / Down     : 5 / 2
Rekeys        : 636
DP Updates    : 0
DPD Cleanups  : 0

            Packets From   Packets To     Packet Errors To     Bytes From      Bytes To
-----------------------------------------------------------------------------------------
BinOS        85              0                                                  0
IOSd         0               0               0                    0             0
TLS Client   0               0               0                    0             0
```

```
Tunnel Statistics

SSL Handshake Init / Done : 641 / 641
TCP Connection Req / Done : 641 / 641
Tunnel Packets
Rx / Tx           : 85 / 0
Injected / Failed : 0 / 0
Consumed          : 0

CSTP Packets
Control Rx / Tx   : 3839 / 3839
Data    Rx / Tx   : 0 / 85
Config Req / Resp : 641 / 641
DPD    Req / Resp : 3198 / 3198
Invalid Rx        : 0

FQDN Counters
Req / Resp / Success : 0 / 0 / 0

NAT Counters
Transalte In / Out : 0 / 0
Ignore    In / Out : 0 / 0
Failed             : 0
Invalid            : 0
No Entry           : 0
Unsupported        : 0

Internal Counters

Type     Allocated    Freed
-----------------------------
EV       1299         1295
Tunnel    5            4
Conn     643           642
Sess      3            2

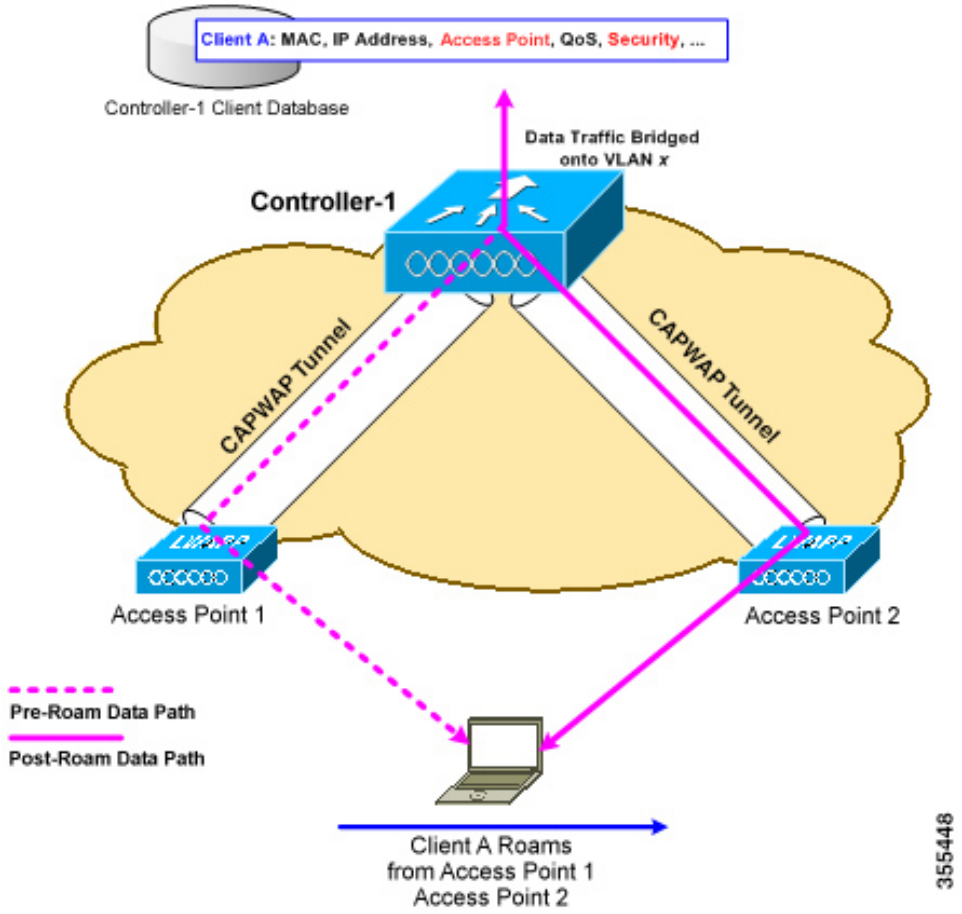
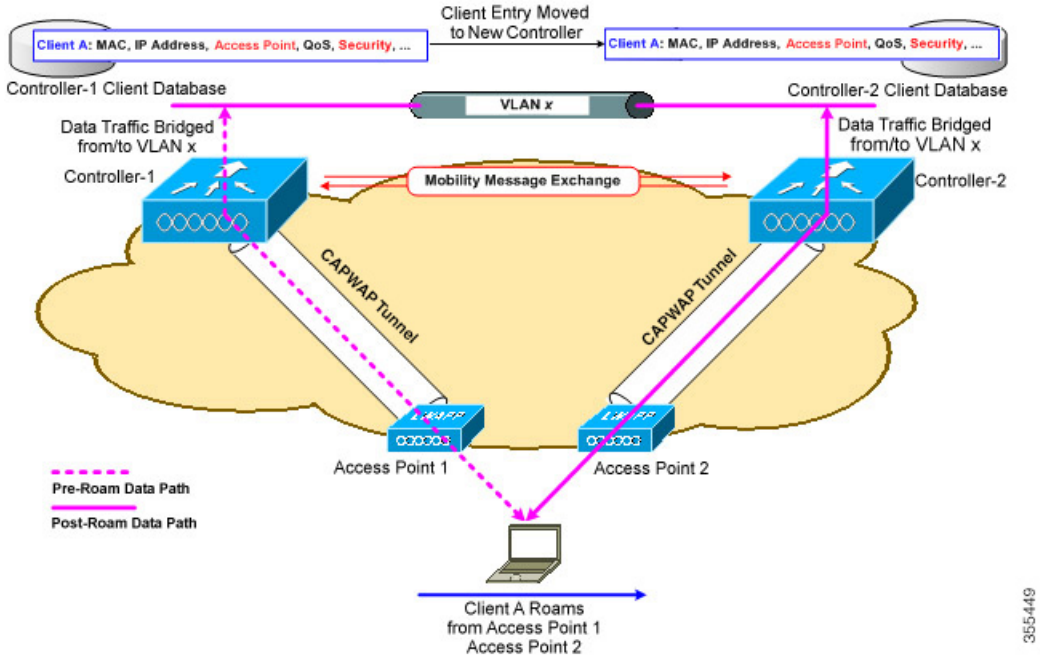
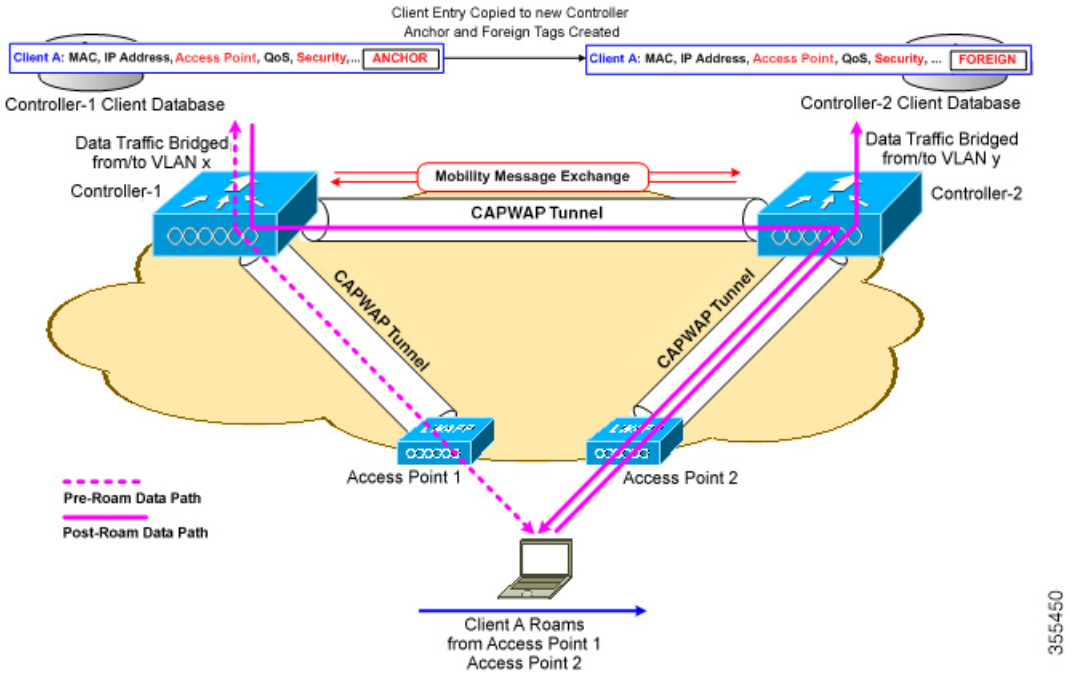
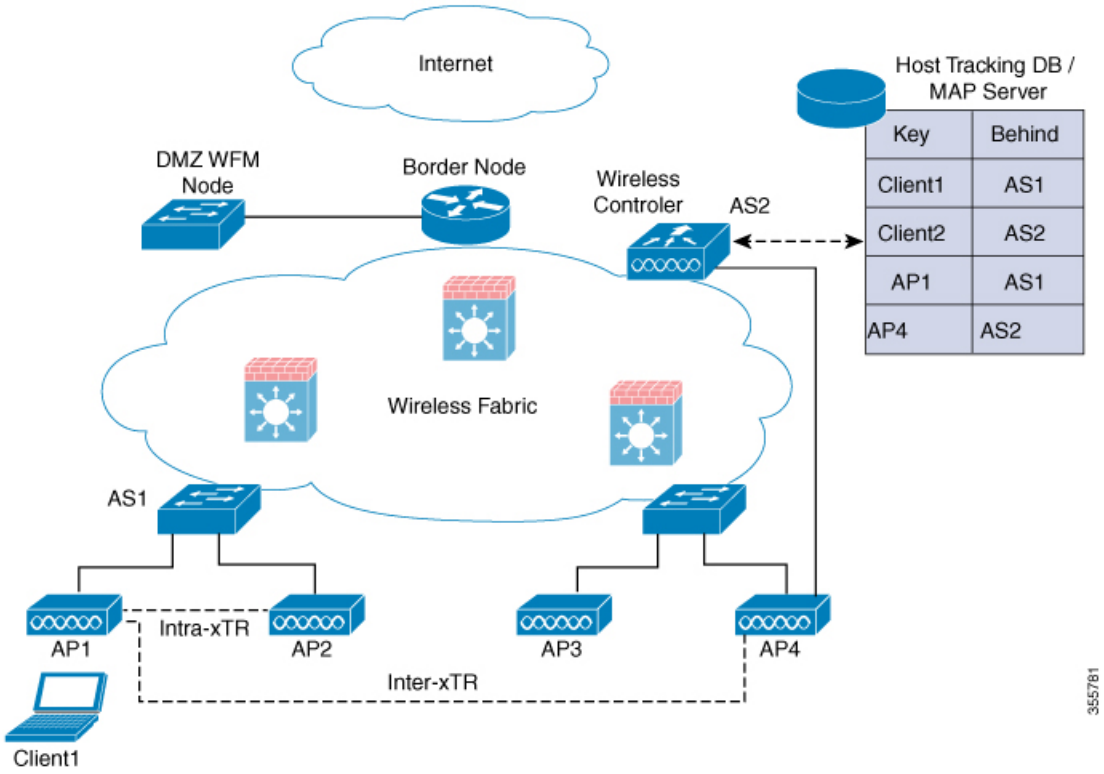
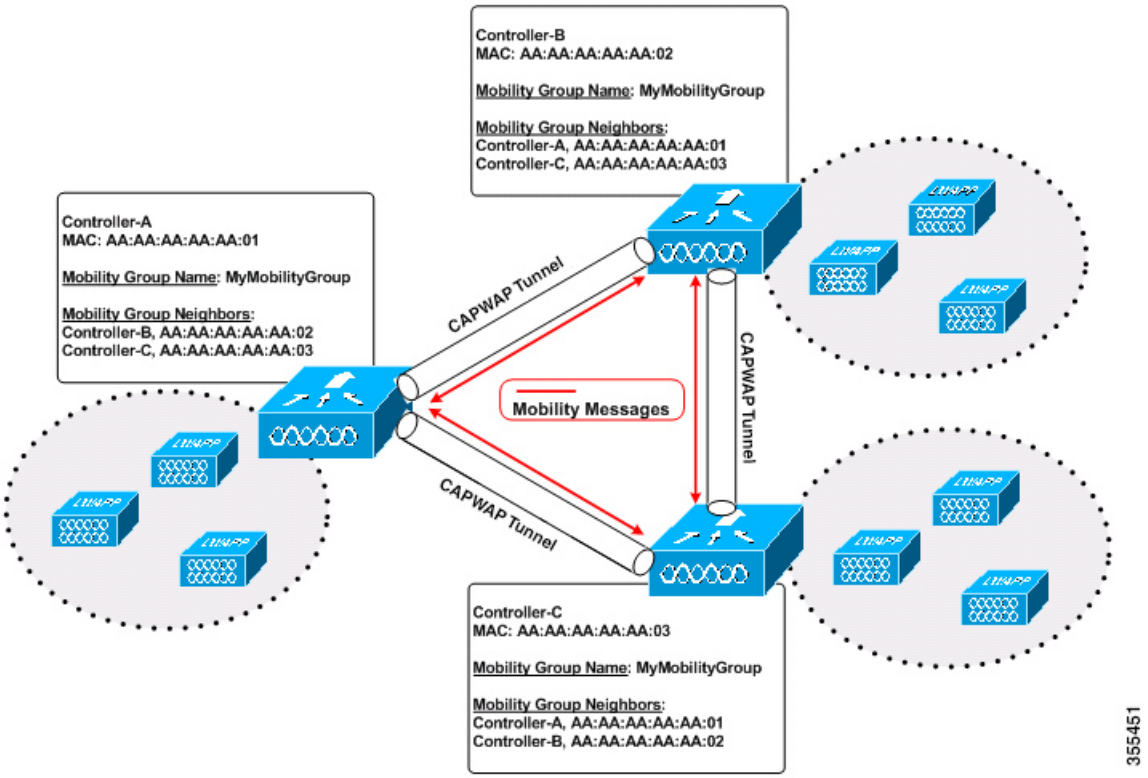
Config Message Related Counters
Type     Success       Failed
------------------------------
Create     3             0
Delete     2             0
```

To view the TLS client-session summary, use the following command.

```
Device# show platform software tlsc session summary

TLS Client - Session Summary

Name     ID     Created            State       Since               Elapsed
-------------------------------------------------------------------------------------------
fqdn     0      04/20/21 00:36:42  Up          04/21/21 20:30:21  9 hours 26 minutes 44
seconds
```

CHAPTER 128

Configuring RFC 5580 Location Attributes

- Feature History for RFC 5580 Location Attributes, on page 1395
- Information About RFC 5580 Location Attributes , on page 1396
- Information About Location-Capable Attribute , on page 1398
- Restriction for Configuring RFC 5580 Location Attributes, on page 1398
- Configuring Location Delivery Based on Out-of-Band Agreement (CLI), on page 1398
- Configuring Location-Capable Attribute (CLI), on page 1399
- Creating Location Attributes, on page 1399
- Associating Location Attributes with User Location (CLI), on page 1403
- Associating Location Attributes with the NAS Location (CLI), on page 1404
- Verifying RFC 5580 Location Attribute Configuration, on page 1405

Feature History for RFC 5580 Location Attributes

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 97: Feature History for RFC 5580 Location Attributes

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	Support for RFC 5580 Location Attributes in the Controller	This feature uses the RFC 5580 location attributes to convey location-related information for authentication and accounting exchanges. The controller supports the following RFC 5580-related attributes: • Location-Information • Location-Data CIVIC Profile: Country • Location-Data CIVIC Profile: CAtype 1 (State) • Location-Data CIVIC Profile: CAtype 3 (City) • Location-Data CIVIC Profile: CAtype 23 (Venue Name) • Location-Data CIVIC Profile: CAtype 24 (Zip Code) • Location-Data GEO Profile (Longitude, Latitude, and Altitude) • Operator Name

Information About RFC 5580 Location Attributes

The RFC 5580 location attributes convey location-related information for authentication and accounting exchanges.

The location information is useful in several scenarios. Wireless networks are deployed in public places, such as shopping malls, airports, hotels, and coffee shops by a diverse set of operators, such as wireless internet service providers (WISPs), cellular network operators, and fixed broadband networks. In all these scenarios, the network may need to know the user location to enable location-aware authorization, billing, or services.

To preserve user privacy, the location information must be protected against unauthorized access and distribution.

The RFC 5580 defines two types of location:

- **User location**: This location is more specific to users.

Note The user location is configured in AP.

- **NAS location**: This is the common location to host all the users. For instance, suppose you configure user location at AP1, other users connecting to AP1 will also have the same user location. Now other users coming from AP2 will have a different user location. Thus, if AP1 and AP2 are connected to the controller, and you configure a NAS location, then users from AP1 and AP2 are connected to the same NAS location.

Note The NAS location is configured in AAA.

You can define certain profiles in each location. Profile refers to the attributes used to define the location. Each location has two profiles, namely, Civic and Geo.

The following are the location profiles:

- **Civic Profile**: In this profile, the location is described in terms of attributes such as Country, State, City, Area, and Postal Code.
- **Geo Profile**: In this profile, the location is described in terms of attributes such as Latitude, Longitude, and Altitude.

For users with both user location and NAS location, you can set their location in both Civic and Geo profile formats. Such users have the following locations:

- Civic User location
- Civic NAS location
- Geo User location
- Geo NAS location

Each location information, for instance, the civic user location, is sent using the following attributes:

- Location-Information
- Location-Data

The controller supports the following RFC 5580-related attributes:

- Location-Information
- Location-Data CIVIC Profile: Country
- Location-Data CIVIC Profile: CAtype 1 (State)
- Location-Data CIVIC Profile: CAtype 3 (City)
- Location-Data CIVIC Profile: CAtype 23 (Venue Name)
- Location-Data CIVIC Profile: CAtype 24 (Zip Code)
- Location-Data GEO Profile (Longitude, Latitude, and Altitude)
- Operator Name

Thus, a user can have four locations and one operator name.

To transfer location information, the Out-of-Band Agreement (Flow 1) delivery method mentioned in RFC 5580 is supported.

This is applicable only if the feature is enabled and location information is configured.

Information About Location-Capable Attribute

Cisco IOS-XE Dublin 17.11.1 supports the Location-Capable feature attribute from RFC 5580. This attribute is sent only in the network access requests. To enable the Location-Capable attribute, configure the **radius-server attribute wireless location delivery out-of-band include-location-capable** command. This attribute informs the RADIUS server that this device can send location information.

The RFC5580 supports three flows or modes of location delivery. As per the RFC, the Location-Capable attribute should be sent in Flow-2, which is location delivery based on Initial-Request. The above-mentioned configuration enables sending this attribute in Flow-1, which is Location delivery based on Out-of-Band agreement as well.

When an authentication or authorization request is received, the Location-Capable feature attribute is added to the request along with other location attributes as per the configuration (explained in the other section). This is applicable only for wireless clients. The RADIUS server might use this information to provide network access.

Restriction for Configuring RFC 5580 Location Attributes

This feature is supported only for 802.1X users.

Configuring Location Delivery Based on Out-of-Band Agreement (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius-server attribute wireless location delivery out-of-band** **Example:** `Device(config)# radius-server attribute wireless location delivery out-of-band`	Configures RFC 5580 Out-of-Band location support.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring Location-Capable Attribute (CLI)

Use the **radius-server attribute wireless location delivery out-of-band** command to enable the feature globally.

You can use the **radius-server attribute wireless location delivery out-of-band include-location-capable** command to include the location-capable attribute along with other location attributes.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius-server attribute wireless location delivery out-of-band include-location-capable** **Example:** `Device(config)# radius-server attribute wireless location delivery out-of-band include-location-capable`	Configures RFC 5580 out-of-band location attributes along with enabling the location-capable attribute to be part of the access request.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Creating Location Attributes

Configuring a Civic Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**location civic-location identifier** *civic_identifier* **Example:** `Device(config)# location civic-location identifier USER_C_1`	Configures the civic profile for User location. Here, *civic_identifier* refers to the civic location identifier string. It can take up to 215 characters. You can enter a total of 250 bytes to configure civic address attributes. Cisco reserves 50 bytes for internal information. Therefore, the

	Command or Action	Purpose
		remaining 200 bytes can be used for user-configured civic location. **Note** You can configure the following types of civic attributes and add them to the RADIUS requests: • Country • City • State • Postal Code • Name
Step 3	**country** *country_ID* **Example:** `Device(config-civic)# country IN`	Sets the country ID. **Note** Only two-letter ISO 3166 country codes are accepted.
Step 4	**city** *city_name* **Example:** `Device(config-civic)# city Bangalore`	Sets the city name.
Step 5	**state** *state_name* **Example:** `Device(config-civic)# state Karnataka`	Sets the state name.
Step 6	**postal-code** *postal_code* **Example:** `Device(config-civic)# postal-code 562016`	Sets the postal code.
Step 7	**name** *residence_name* **Example:** `Device(config-civic)# name Nivas`	Sets the residence name.
Step 8	**end** **Example:** `Device(config-civic)# end`	Returns to privileged EXEC mode.

Configuring a Geo Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**location geo-location identifier** *geo_identifier* **Example:** `Device(config)# location geo-location identifier USER_G_1`	Configures a Geo profile for user location. Here, *geo_identifier* refers to the geographic location identifier string. It can take up to 215 characters.
Step 3	**latitude** *latitude_in_degrees* **resolution** [*resolution_value*] **Example:** `Device(config-geo)# latitude "34 12 15"`	Sets the latitude information. The optional parameters are documented within square brackets. While configuring the latitude, you can specify the resolution, in meters. If you do not specify any resolution, a default value of 10 meters is used.
Step 4	**longitude** *longitude_in_degrees* **resolution** *resolution_value* **Example:** `Device(config-geo)# longitude "111 59 44"`	Sets the longitude information. The optional parameters are documented within square brackets. While configuring the longitude, you can specify the resolution, in meters. If you do not specify any resolution, a default value of 10 meters is used.
Step 5	**altitude** *altitude_value* {**feet resolution** *resolution_value* | **floor** | **meters resolution** *resolution_value*} **Example:** `Device(config-geo)# altitude 10 meters resolution 10`	Configures the altitude for the geographic location. The optional parameters are documented within square brackets. • *altitude_value*: Refers to the altitude, in feet, floors, or meters. • *resolution_value*: Refers to the resolution, in feet or meters. **Note** Both the altitude and the altitude resolution must be in the same unit.
Step 6	**resolution** *resolution_value* **Example:** `Device(config-geo)# resolution 30`	Specifies a single common resolution for latitude and longitude.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-geo)# end`	Returns to privileged EXEC mode.

Configuring an Operator Name (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**location operator identifier** *identifier_name* **Example:** `Device(config)# location operator identifier USER_O_1`	Configures an operator name for the user location. Here, *identifier_name* supports strings up to 215 characters in length.
Step 3	**name** *operator-name* **Example:** `Device(config-operator)# name ACT`	Configures the location operator name. Here, *operator-name* supports strings up to 248 characters in length.
Step 4	**namespace-id** {**E212** | **ICC** | **REALM** | **TADIG**} **Example:** `Device(config-operator)# namespace-id ICC`	Configures the namespace for a location. The following are the namespace options: • **E212**: Refers to the Mobile Country Code (MCC) and Mobile Network Code (MNC). • **ICC**: Refers to the International Telecommunication Union Carrier Codes (ICC). • **REALM**: Refers to any registered domain name. • **TADIG**: Refers to the Transferred Account Data Interchange Group (TADIG) code.

	Command or Action	Purpose
		Note • If you have not configured any namespace, **REALM** is used as the default value. • The operator name can be associated with both NAS-Location and USER-Location. When an operator name is configured at both the locations, the operator name that is configured in USER-Location takes precedence.
Step 5	**end** **Example:** `Device(config-operator)# end`	Returns to privileged EXEC mode.

Associating Location Attributes with User Location (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap location name** *location_name* **Example:** `Device(config)# ap location name OFFICE`	Configures a location name for an AP.
Step 3	**ap-eth-mac** *AP_Ethernet_MAC* **Example:** `Device(config-ap-location)# ap-eth-mac 0a0b.0cf0.0001`	Adds the AP to the location. Here, *AP_Ethernet_MAC* refers to the AP Ethernet MAC address.
Step 4	**location civic-location-id** *identifier_name* **Example:** `Device(config-ap-location)# location civic-location-id USER_C_1`	Associates the civic location attribute with the user location.
Step 5	**location geo-location-id** *identifier_name* **Example:**	Associates the geographic location attribute with the user location.

	Command or Action	Purpose
	`Device(config-ap-location)# location geo-location-id USER_G_1`	
Step 6	**location operator-id** *identifier_name* **Example:** `Device(config-ap-location)# location operator-id USER_O_1`	Associates the operator location attribute with the user location.
Step 7	**end** **Example:** `Device(config-ap-location)# end`	Returns to privileged EXEC mode.

Associating Location Attributes with the NAS Location (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**radius-server attribute wireless location civic-location-id** *identifier_name* **Example:** `Device(config)# radius-server attribute wireless location civic-location-id NAS_C_1`	Associates the civic location attribute with the NAS location. Here, *identifier_name* supports strings up to 215 characters in length.
Step 3	**radius-server attribute wireless location geo-location-id** *identifier_name* **Example:** `Device(config)# radius-server attribute wireless location geo-location-id NAS_G_1`	Associates the geographic location attribute with the NAS location. Here, *identifier_name* supports strings up to 215 characters in length. Enter a valid or existing identifier name.
Step 4	**radius-server attribute wireless location operator-id** *identifier_name* **Example:** `Device(config)# radius-server attribute wireless location operator-id NAS_0_1`	Associates the operator location attribute with the NAS location.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying RFC 5580 Location Attribute Configuration

To verify the location attributes associated with a given location, use the following command:

```
Device# show ap location details AAA_location
Location Name.....................: AAA_location
Location description..............:
Policy tag........................: default-policy-tag
Site tag..........................: default-site-tag
RF tag............................: default-rf-tag
AAA Location Status ..............: Enabled
Civic Location Identifier : NAS_C_1
Geo Location Identifier   : NAS_G_1
Operator Name Identifier  : NAS_O_1

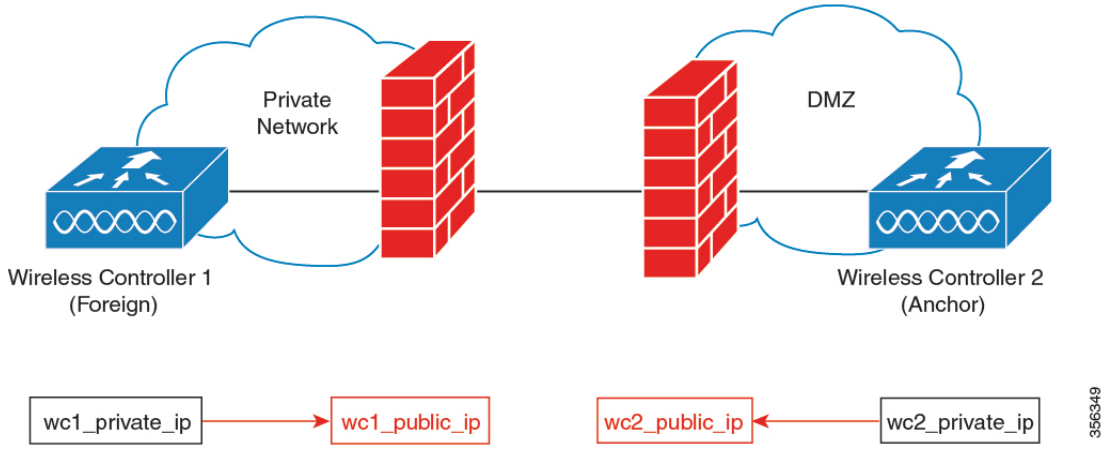
Configured list of APs
38ed.18ca.5a20
```

To verify the Cisco AP location, use the following command:

```
Device# show ap name AP38ED.18CA.5A20 config general
Cisco AP Name   : AP38ED.18CA.5A20
================================================

Cisco AP Identifier                             : 38ed.18cb.cf00
Country Code                                    : Multiple Countries :
Regulatory Domain Allowed by Country            : 802.11bg:   802.11a:   802.11 6GHz:
AP Country Code                                 : US  -
AP Regulatory Domain
  802.11bg                                      : -A
  802.11a                                       : -A
MAC Address                                     : 38ed.18ca.5a20
IP Address Configuration                        : Static IP assigned
IP Address                                      : 9.4.172.111
IP Netmask                                      : 255.255.255.0
Gateway IP Address                              : 9.4.172.1
Fallback IP Address Being Used                  :
Domain                                          :
Name Server                                     :
CAPWAP Path MTU                                 : 1485
Capwap Active Window Size                       : 1
Telnet State                                    : Disabled
CPU Type                                        :  ARMv7 Processor rev 0 (v7l)
Memory Type                                     : DDR3
Memory Size                                     : 995328 KB
SSH State                                       : Disabled
Cisco AP Location                               : AAA_location
-
-
-
```

To verify the location attributes associated with a given MAC address, use the following command:

```
Device# show wireless client mac 0080.5222.545c detail

Client MAC Address : 0080.5222.545c
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
AP MAC Address : 38ed.18cb.cf00
AP Name: AP38ED.18CA.5A20
AP slot : 1
Client State : Associated
```

```
Policy Profile : default-policy-profile
Flex Profile : N/A
…
Civic Location Identifier : NAS_C_1
Geo Location Identifier   : NAS_G_1
Operator Name Identifier  : NAS_O_1
```

Note You will be able to view this output only if the RFC 5580 feature is enabled.

To verify the Civic location details, use the following command:

```
Device# show location civic-location identifier TEST1
Civic location information
--------------------------
Identifier              : TEST1
Name                    : home
City                    : Morges
State                   : Vaud
Postal code             : 1110
Country                 : CH
```

To verify the Geo location details, use the following command:

```
Device# show location geo-location identifier TEST4
Geo location information
------------------------
Identifier  : TEST4
Latitude    : 46.5112700
Longitude   : 6.4985400
Altitude    : 380 meters          Resolution : 10
Resolution  : 100
```

To verify the Operator location details, use the following command:

```
Device# show location operator-location identifier myoperator
Operator location information
-----------------------
Operator Identifier     : myoperator
Operator Name           : myoperator
Operator Namespace      : REALM
------------------------
```

CHAPTER 129

IP MAC Binding

- Information About IP MAC Binding, on page 1407
- Use Cases for No IP MAC Binding, on page 1407
- Disabling IP MAC Binding (CLI), on page 1408
- Verifying IP MAC Binding, on page 1408

Information About IP MAC Binding

The wireless device tracking features, such as, theft detection, proxy, DHCP relay, gleaning, and suppression are enabled with IP MAC address binding configuration.

Note The IP MAC address binding is enabled by default in the policy profile.

No IP MAC Binding

It disables all the wireless device tracking features for wireless clients' IPv4 address.

Note It is not normally necessary to disable IP MAC binding, except for the following scenarios:

- When you have a single wireless station with multiple IP addresses.
- When you intentionally have duplicate IP addresses across clients.
- When you are using ARP-spoofing Network Access Control (NAC) devices.

Use Cases for No IP MAC Binding

The following are the use cases for No IP MAC binding:

- Disabling IP Learning in FlexConnect Mode
- Disabling Device Tracking to Support NAC Devices

- Disabling IP Learning in FlexConnect Mode

Disabling IP MAC Binding (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy test-profile-policy`	Configures the wireless profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the wireless policy profile. **Note** Disabling policy profile results in associated AP and client to rejoin.
Step 4	**no ip mac-binding** **Example:** `Device(config-wireless-policy)# no ip mac-binding`	Disables IP MAC binding.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 6	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to privileged EXEC mode.

Verifying IP MAC Binding

To verify if the IP MAC binding is disabled or not, use the following command:

```
Device# show run | b wireless profile policy test-profile-policy
wireless profile policy test-profile-policy
 no ip mac-binding
 vlan VLAN0169
```

CHAPTER 130

Disabling IP Learning in FlexConnect Mode

- Information About Disabling IP Learning in FlexConnect Mode, on page 1409
- Restrictions for Disabling IP Learning in FlexConnect Mode, on page 1409
- Disabling IP Learning in FlexConnect Mode (CLI), on page 1410
- Verifying MAC Entries from Database, on page 1410

Information About Disabling IP Learning in FlexConnect Mode

In FlexConnect local switching scenarios, where clients from the same sites may share the same address range, there is a possibility of multiple clients being allocated or registered with the same IP address. The controller receives IP address information from the AP, and if more than one client attempts to use the same IP address, the controller discards the last device trying to register an already-used address as an IP theft event, potentially resulting in client exclusion.

The Disabling IP learning in FlexConnect mode feature utilizes the **no ip mac-binding** command to ensure that no device tracking is done for clients, thus preventing the IP theft error.

Note

- This feature is applicable only for IPv4 addresses.
- Configuring **ip overlap** in FlexConnect Profile assists overlapping IP address support for clients across different sites in FlexConnect local switching.

Restrictions for Disabling IP Learning in FlexConnect Mode

- The **wireless client ip deauthenticate** command works by referring to the IP table binding entries directly. It does not work for client whose IPs are not learnt.
- Overlapping IP addresses within a single site tag and across different site tags require different settings. Furthermore, if a single site tag contains overlapping IP addresses, L3 web authentication is necessary. However, L3 web authentication relies on IP addresses, and ensuring the uniqueness of IP addresses cannot be guaranteed, making this combination incorrect.
- When IP Source Guard (IPSG) is enabled and multiple binding information is sent with the same IP and preference level (such as DHCP, ARP, and so on) to CPP, the CPP starts to ignore the later bindings

after the first binding creation. Hence, you should not configure IPSG and disable IP MAC binding together. If IPSG and **no ip mac-binding** are configured together then IPSG does not work.

Disabling IP Learning in FlexConnect Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy test-profile-policy`	Configures the wireless profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the wireless policy profile. **Note** Disabling policy profile results in associated AP and client to rejoin.
Step 4	**no ip mac-binding** **Example:** `Device(config-wireless-policy)# no ip mac-binding`	Disables IP learning in FlexConnect mode.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 6	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to privileged EXEC mode.

Verifying MAC Entries from Database

To verify the MAC details from database, use the following command:

```
Device# show wireless device-tracking database mac
MAC VLAN IF-HDL IP
------------------------------------------------------------------------------------------------------
6c96.cff2.889a 64 0x90000008 9.9.64.175
```

CHAPTER 131

Disabling Device Tracking to Support NAC Devices

- Feature History for Disabling Device Tracking to Support NAC Devices, on page 1411
- Information About Disabling Device Tracking to Support NAC Devices, on page 1411
- Restrictions for Disabling Device Tracking to Support NAC Devices, on page 1412
- Disabling Device Tracking for Wireless Clients (CLI), on page 1412
- Verifying ARP Broadcast, on page 1413

Feature History for Disabling Device Tracking to Support NAC Devices

This table provides release and related information for the feature explained in this module.

Table 98: Feature History for Disabling Device-Tracking to Support NAC Devices

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	Disabling Device Tracking to Support NAC Devices	This feature helps to control the flow of traffic between wireless clients using network access control (NAC) device.

Information About Disabling Device Tracking to Support NAC Devices

The feature helps to control the flow of traffic between wireless clients using a network access control (NAC) device. The NAC device blocks the direct traffic between wireless clients using ARP spoofing.

Use the **no ip mac-binding** command for ARP spoofing from the NAC and disabling the wireless client device tracking.

Note This feature is applicable only for IPv4 addresses.

Restrictions for Disabling Device Tracking to Support NAC Devices

- The **wireless client ip deauthenticate** command works by referring to the IP table binding entries directly. It does not work for client whose IPs are not learnt.
- Layer 3 web authentication and other L3 policies are not supported.
- When IP Source Guard (IPSG) is enabled and multiple binding information is sent with the same address and preference level (such as DHCP, ARP, and so on) to Cisco Packet Processor (CPP), the CPP starts to ignore the later bindings after the first binding creation. Hence, you should not configure IPSG and **no ip mac-binding** together. If IPSG and **no ip mac-binding** are configured together then IPSG does not work.

Disabling Device Tracking for Wireless Clients (CLI)

Disable device tracking for wireless clients using commands.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy test-profile-policy`	Configures the wireless profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the wireless policy profile. **Note** Disabling policy profile results in associated AP and client to rejoin.
Step 4	**no ip mac-binding** **Example:** `Device(config-wireless-policy)# no ip mac-binding`	Disables the IP-MAC address binding.

	Command or Action	Purpose
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 6	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to privileged EXEC mode.
Step 7	**vlan configuration** *vlan-id* **Example:** `Device(config)# vlan configuration 20`	Configures a VLAN and enters VLAN configuration mode.
Step 8	**arp broadcast** **Example:** `Device(config-vlan-config)# arp broadcast`	Enables ARP broadcast on VLAN.
Step 9	**end** **Example:** `Device(config-vlan-config)# end`	Returns to privileged EXEC mode.

Verifying ARP Broadcast

To verify the ARP broadcast, use the following command:

```
Device# show platform software arp broadcast
Arp broadcast is enabled on vlans:
20,50
```

PART VIII

Mobility

- Mobility, on page 1417
- NAT Support on Mobility Groups, on page 1437
- Static IP Client Mobility, on page 1441
- Mobility Domain ID - Dot11i Roaming, on page 1445
- 802.11r Support for Flex Local Authentication, on page 1447
- Opportunistic Key Caching, on page 1449

CHAPTER 132

Mobility

- Introduction to Mobility, on page 1417
- Guidelines and Restrictions, on page 1422
- Configuring Mobility (GUI), on page 1424
- Configuring Mobility (CLI), on page 1425
- Configuring Inter-Release Controller Mobility (GUI), on page 1427
- Configuring Inter-Release Controller Mobility, on page 1427
- Verifying Mobility, on page 1431

Introduction to Mobility

Mobility or roaming is a wireless LAN client's ability to maintain its association seamlessly from one access point to another access point securely and with as little latency as possible. This section explains how mobility works when controllers are included in a wireless network.

When a wireless client associates and authenticates to an access point, the access point's controller places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated access point. The controller uses this information to forward frames and manage traffic to and from a wireless client.

Figure 40: Intracontroller Roaming

This figure shows a wireless client that roams from one access point to another access point when both access points are joined to the same controller.



When a wireless client moves its association from one access point to another access point, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an access point joined to one controller to an access point joined to a different controller. It also varies based on whether the controllers are operating on the same subnet.

Figure 41: Intercontroller Roaming

This figure shows intercontroller roaming, which occurs when the wireless LAN interfaces of controllers are on the same IP subnet.



When a client joins an access point associated with a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains transparent to the user.

Note All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication in order to comply with the IEEE standard.

Important Intersubnet Roaming is not supported for SDA.

Figure 42: Intersubnet Roaming

This figure shows intersubnet roaming, which occurs when the wireless LAN interfaces of controllers are on different IP subnets.



Intersubnet roaming is similar to intercontroller roaming in that, controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an *anchor* entry in its own client database. The database entry is copied to the new controller client database and marked with a *foreign* entry in the new controller. The roam remains transparent to the wireless client, and the client maintains its original IP address.

In intersubnet roaming, WLANs on both anchor and foreign controllers should have the same network access privileges, and no source-based routing or source-based firewalls in place. Otherwise, the clients may have network connectivity issues after the handoff.

In a static anchor setup using controllers and a RADIUS server, if AAA override is enabled to dynamically assign VLAN and QoS, the foreign controller updates the anchor controller with the right VLAN after a Layer 2 authentication (802.1x). For Layer 3 RADIUS authentication, the RADIUS requests for authentication are sent by the anchor controller.

Note The Cisco Catalyst 9800 Series Wireless Controller mobility tunnel is a CAPWAP tunnel with control path (UDP 16666) and data path (UDP 16667). The control path is DTLS encrypted by default. Data path DTLS can be enabled when you add the mobility peer.

SDA Roaming

SDA supports two additional types of roaming, which are Intra-xTR and Inter-xTR. In SDA, xTR stands for an access-switch that is a fabric edge node. It serves both as an ingress tunnel router as well as an egress tunnel router.

When a client on a fabric enabled WLAN, roams from an access point to another access point on the same access-switch, it is called Intra-xTR. Here, the local client database and client history table are updated with the information of the newly associated access point.

When a client on a fabric enabled WLAN, roams from an access point to another access point on a different access-switch, it is called Inter-xTR. Here, the map server is also updated with the client location (RLOC) information. Also, the local client database is updated with the information of the newly associated access point.

Figure 43: SDA Roaming

This figure shows inter-xTR and intra-xTR roaming, which occurs when the client moves from one access point to another access point on the same switch or to a different switch in a Fabric topology.



Definitions of Mobility-related Terms

- Point of Attachment—A station's point of attachment is where its data path is initially processed upon entry into the network.
- Point of Presence—A station's point of presence is the place in the network where the station is being advertised.
- Station—A user's device that connects to and requests service from a network.

Mobility Groups

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers

in a network to dynamically share information and forward data traffic when intercontroller or intersubnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support intercontroller wireless LAN roaming and controller redundancy.

Note While moving an AP from one controller to another (when both controllers are mobility peers), a client associated to controller-1 before the move might stay there even after the move. This is due to a timeout period on controller-1, where the client entry is maintained (for the purposes of roaming/re-association scenarios). To avoid the client being anchored in controller-1, remove the mobility peer configuration of the controller.

Figure 44: Example of a Single Mobility Group



As shown in the figure above, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message (or multicast message if mobility multicast is configured) to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client.

Guidelines and Restrictions

The following AireOS and Cisco Catalyst 9800 Series Wireless Controller platforms are supported for SDA Inter-Controller Mobility (AireOS controller–to-Cisco Catalyst 9800 Series Wireless Controller):

- **AireOS**

- Cisco 3504
- Cisco 5520
- Cisco 8540

- **Cisco Catalyst 9800 Series Wireless Controller**
  - Cisco Catalyst 9800 Wireless Controller for Cloud
  - Cisco Catalyst 9800-80 Wireless Controller
  - Cisco Catalyst 9800-40 Wireless Controller
  - Cisco Catalyst 9800-L Wireless Controller

The following controller platforms are supported for SDA Inter-Controller Mobility:

- **Catalyst Switches**
  - Cisco 9300

- **Cisco Catalyst 9800 Series Wireless Controller**
  - Cisco Catalyst 9800 Wireless Controller for Cloud
  - Cisco Catalyst 9800-40 Wireless Controller

- Ensure that the data DTLS configuration on the Cisco Catalyst 9800 Series Wireless Controller and AireOS are the same, as configuration mismatch is not supported on the Cisco Catalyst 9800 Series Wireless Controller and it causes the mobility data path to go down.
- In intercontroller roaming scenarios, policy profiles having different VLANs is supported as a Layer 3 roaming.
- In AireOS controller, L3 override is not supported in guest VLAN. Hence, the client does not trigger DHCP Discovery on the new VLAN automatically.
- Policy profile name and client VLAN under policy profile can be different across the controllers with the same WLAN profile mapped.
- In intracontroller roaming scenarios, client roaming is supported between same policy profiles, with WLAN mapped.

  From Cisco IOS XE Amsterdam 17.3.x, The controller allows seamless roaming between same WLAN associated with different policy profile. For more information, see Client Roaming Policy Profile feature.
- If a client roams in web authentication state, the client is considered as a new client on another controller instead of being identified as a mobile client.
- Controllers that are mobility peers must use the same DHCP server to have an updated client mobility move count on intra-VLAN.
- Data DTLS and SSC hash key must be same for mobility tunnels between members.
- Mobility move count is updated under client detail only during inter-controller roaming. Intra-controller roaming can be verified under client stats and mobility history.

- Anchor VLAN in Cisco Catalyst 9800 Series Wireless Controller is represented as Access VLAN on the Cisco AireOS controller.
- When clients are roaming, their mobility role is shown as *Unknown*. This is because the roaming clients are in *IP learn* state, and in such a scenario, there are many client additions to the new instance and deletions in the old instance.
- In inter-controller roaming between 9800 and 9800/AireOS, client roaming is not supported, whenever there is a WLAN profile mismatch.
- Only IPv4 tunnel is supported between Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS controller.
- Ensure that you configure the mobility MAC address using the **wireless mobility mac-address** command for High-Availability to work.
- Mobility tunnel will not work if ECDSA based certificate or trustpoint is used for wireless management.
- If Anchor and Foreign controllers are put in the same Layer 2 network, it creates a loop topology (one path is Layer 3 mobility tunnel between Anchor and Foreign, another path is Layer 2 wired connection between Anchor and Foreign). In this topology, MAC_CONFLICT warning message can be seen on both the Anchor and Foreign controllers. This MAC_CONFLICT warning message is printed once every minute. However, it doesn't have any functionality and performance impact. As a best practice, do not use management VLAN as client VLAN.
- Mobility Tunnel will go down and come up if SSO is triggered due to gateway check failure.
- If the current AP has 5-GHz slot2 radio on L2 and L3 mobility 5-GHz slot2, the WLAN BSSID is only added to the 11k or 11v neighbor information. As a result, the AP does not have the information of radio properties of the APs belonging to the other controllers. Hence, it can be assumed that the radio properties of the APs belonging to the other controllers are similar to that of the current AP. If the current AP does not have slot2, the other APs cannot be added as a neighbor. In such a scenario, the validation fails and does not add this radio to the neighbor list.
- We recommend that you use the default keepalive count and interval values to reduce convergence time between the Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers while setting up a mobility tunnel.
- A new client may take up to 3 seconds to join the network when the mobility tunnel is UP and mobility peers are configured. This is because the system sends three mobile messages (one second apart) to find out whether the client is already part of the network.

Configuring Mobility (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mobility**.
The **Wireless Mobility** page is displayed on which you can perform global configuration and peer configuration.

Step 2 In the **Global Configuration** section, perform the following tasks:

a) Enter a name for the mobility group.
b) Enter the multicast IP address for the mobility group.

c) In the **Keep Alive Interval** field, specify the number of times a ping request is sent to a mobility list member before the member is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.
d) Specify the **Mobility Keep Alive Count** amount of time (in seconds) between each ping request sent to a mobility list member. The valid range is 1 to 30 seconds.
e) Enter the DSCP value for the mobility group.
f) Enter the mobility MAC address.
g) Click **Apply**.

Step 3 In the **Peer Configuration** tab, perform the following tasks:

a) In the **Mobility Peer Configuration** section, click **Add**.
b) In the **Add Mobility Peer** window that is displayed, enter the MAC address and IP address for the mobility peer. The MAC address can be either in *xx:xx:xx:xx:xx:xx*, *xx-xx-xx-xx-xx-xx*, or *xxxx.xxxx.xxxx* format.
c) Additionally, when NAT is used, enter the optional public IP address to enter the mobility peer's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility peer's direct IP address.
d) Enter the mobility group to which you want to add the mobility peer.
e) Select the required status for **Data Link Encryption**.
f) Specify the **SSC Hash** as required.

SSC hash is required if the peer is a Cisco Catalyst 9800-CL Wireless Controller, which uses self-signed certificate and hence SSC hash is used as an additional validation. SSC hash is not required if peer is an appliance, which will have manufacturing installed certificates (MIC) or device certificates burned in the hardware.

g) Click **Save & Apply to Device**.
h) In the **Non-Local Mobility Group Multicast Configuration** section, click **Add**.
i) Enter the mobility group name.
j) Enter the multicast IP address for the mobility group.
k) Click **Save**.

Configuring Mobility (CLI)

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group-name* **Example:** `Device(config)# wireless mobility group name Mygroup`	Creates a mobility group named **Mygroup**.
Step 2	**wireless mobility mac-address** *mac-addr* **Example:** `Device(config)# wireless mobility mac-address 00:0d:ed:dd:25:82`	Configures the MAC address to be used in mobility messages.

	Command or Action	Purpose
Step 3	**wireless mobility dscp** *value-0-to-63* **Example:** `Device(config)# wireless mobility dscp 10`	(Optional) Configures mobility intercontroller DSCP value.
Step 4	**wireless mobility group keepalive interval** *time-in-seconds* **Example:** `Device(config)# wireless mobility group keepalive interval 5`	(Optional) Configures the interval between two keepalives sent to a mobility member. Valid range is between 1 and 30 seconds. **Note** For controllers connected through mobility tunnels, ensure that both controllers have the same keepalive interval value.
Step 5	**wireless mobility group keepalive count** *count* **Example:** `Device(config)# wireless mobility group keepalive count 3`	(Optional) Configures the keepalive retries before a member status is termed DOWN.

Step 6	Use the options given below to configure IPv4 or IPv6.
	• **wireless mobility mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name* **data-link-encryption**
	• **wireless mobility mac-address** *mac-address* **ip** *peer-ip-address* **public-ip** *public-ip-address* **group** *group-name*
	Example:
	`Device(config#) wireless mobility mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test-group data-link-encryption`
	`Device(config#) wireless mobility mac-address 001E.BD0C.5AFF ip fd09:9:2:49::55 public-ip fd09:9:2:49::55 group scalemobility`
		Adds a peer IPv4 or IPv6 address to a specific group.
		To remove the peer from the local group, use the **no** form of this command.

Step 7	**wireless mobility multicast** {**ipv4** | **ipv6** } *ip-address* or **wireless mobility group multicast-address** *group-name* {**ipv4** | **ipv6** } *ip-address*
	Example:
	`Device(config)# wireless mobility multicast ipv4 224.0.0.4`
	Example:
	`Device(config)# wireless mobility group multicast-address Mygroup ipv4 224.0.0.5`
		(Optional) Configures a multicast IPv4 or IPv6 address for a local mobility group or a nonlocal mobility group.
		Note **Mobility Multicast**—The controller sends a multicast message instead of a unicast message to all the members in the mobility local group or a nonlocal group when a client joins or roams.

	Command or Action	Purpose
		Configures the multicast IPv4 address as 224.0.0.4 for a local mobility group. Configures the multicast IPv4 address as 224.0.0.5 for a nonlocal mobility group.

Configuring Inter-Release Controller Mobility (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mobility** > **Global Configuration**.

Step 2 Enter the **Mobility Group Name**, **Multicast IPv4 Address**, **Multicast IPv6 Address**, **Keep Alive Interval (sec)**, **Mobility Keep Alive Count**, **Mobility DSCP Value** and **Mobility MAC Address**.

Step 3 Click **Apply**.

Configuring Inter-Release Controller Mobility

Inter-Release Controller Mobility (IRCM) is a set of features and functionality that enable interworking between controllers running different software releases. IRCM enables seamless mobility and wireless services across controllers running Cisco AireOS and Cisco IOS (for example, Cisco 8540 WLC to Cisco Catalyst 9800 Series Wireless Controller) for features such as Layer 2 and Layer 3 roaming and guest access or termination.

Note To configure IRCM for different combination of AireOS and Catalyst 9800 controllers, see the Cisco Catalyst 9800 Wireless Controller-Aireos IRCM Deployment Guide.

Follow the procedure described to configure mobility peers on the controller:

Before you begin

The Inter-Release Controller Mobility (IRCM) feature is supported by the following Cisco Wireless Controllers.

- For IRCM deployment, we recommended that you configure:
  - Both Cisco AireOS and Cisco Catalyst 9800 Series Controllers as static RF leaders to avoid RF grouping between them.
  - Configure the same RF network name on both the controllers.
- Cisco Catalyst 9800 Series Wireless Controller platforms running Cisco IOS XE Software version 16.10.1 or later.

- Supports the following Cisco AireOS Wireless Controllers running Cisco AireOS 8.5.14x.x IRCM image based on the 8.5 Maintenance Release software:
  - Cisco 3504 Wireless Controllers
  - Cisco 5508 Wireless Controllers
  - Cisco 5520 Wireless Controllers
  - Cisco 8510 Wireless Controllers
  - Cisco 8540 Wireless Controllers
- By design, Cisco Catalyst 9800 Wireless Controllers does not have the Primary Mode configuration exposed that is to be sent in the Discovery Response. The controller always sends the Discovery Response with the Primary Mode enabled.
- Supported Cisco AireOS Wireless Controllers running AireOS 8.8.111.0 and later. The following controllers are supported:
  - Cisco 3504 Wireless Controllers
  - Cisco 5520 Wireless Controllers
  - Cisco 8540 Wireless Controllers

Note If the peer Cisco Catalyst 9800 Series Wireless Controller is virtual, configure the hash using command:

```
config mobility group member hash 172.20.227.73
3f93a86cee2039e9c3aada1822ad74b89fea30c1
```

```
config mobility group member hash 172.20.227.73
3f93a86cee2039e9c3aada1822ad74b89fea30c1
```

Optionally enable data tunnel encryption using command:

```
config mobility group member data-dtls 00:0c:29:a8:d5:77
enable/disable
```

The hash configure above can be obtained by running the following command on the Cisco Catalyst 9800 Series Wireless Controller:

```
show wireless management trustpoint
Trustpoint Name : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 3f93a86cee2039e9c3aada1822ad74b89fea30c1
Private key Info : Available
```

- The IRCM feature is not supported on the following Cisco AireOS Wireless Controllers:
  - Cisco 2504 Wireless Controllers

- Cisco Flex 7510 Wireless Controllers
- Cisco WiSM 2

- IPv6 is not supported for SDA IRCM for fabric client roaming. IPv6 is supported for IRCM for non-fabric client roaming.
- Ensure that you use AireOS controller that supports Encrypted Mobility feature.
- AVC is not supported for IRCM.
- In mixed deployments (Catalyst 9800 and AireOS Controllers), the WLAN profile name and the policy profile name must be the same. This is due to AireOS not knowing about the policy profile and therefore only sends or receives the WLAN name as both the policy profile and WLAN profile.
- Mobility group multicast is not supported because AireOS does not support mobility multicast in encrypted mobility.
- There could be instances where the total number of clients count shown may be more than those supported on the roaming scale. This inconsistency is observed when the client roaming rate is very high, as the system requires time to update the records. Here, the clients presented on multiple WNCds for a very short time are counted more than once. We recommend that you provide sufficient time for the process to obtain a consistent data before using one of the following methods: show CLIs, WebUI, Cisco Catalyst Center, or SNMP.
- Link Local bridging is not supported. Ensure that you disable it also on the peer AireOS controller.
- IRCM is not supported in FlexConnect and FlexConnect+Bridge modes.

The following client features support IPv6 client mobility between AireOS controllers and Cisco Catalyst 9800 Series Wireless Controller: Accounting, L3 Security (Webauth), Policy (ACL and QoS), IP address assignment and learning through SLAAC and DHCPv6, IPv6 Source Guard, multiple IPv6 address learning, IPv6 multicast, and SISF IPv6 features (RA Guard, RA Throttling, DHCPv6 Guard, and ND Suppress).ß

The following IPv6 features are not supported on Cisco Catalyst 9800 Series Wireless Controller:

- Configurable IPv6 timers
- RA Guard enabled on AP
- Global IPv6 disable

Note

- IPv6 CWA is not supported for both AireOS controllers and Cisco Catalyst 9800 Series Wireless Controller.
- Only eight IPv6 addresses are supported per client.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	Use the options given below to configure IPv4 or IPv6.
	• **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip* **group** *group-name***data-link-encryption**
	• **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip-address* **public-ip** *public-ip-address* **group** *group-name*
	Example:
	`Device(config#) wireless mobility group member mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test-group data-link-encryption`
	`Device(config#) wireless mobility group member mac-address 001E.BD0C.5AFF ip fd09:9:2:49::55 public-ip fd09:9:2:49::55 group scalemobility`
		Adds a peer IPv4 or IPv6 address to a specific group.
		To remove the peer from the local group, use the **no** form of this command.

Step 3	**wireless mobility group name** *group-name* **Example:** `Device(config#) wireless mobility group name test-group`	Adds a name for the local group. The default local group name is "default".
Step 4	**wireless mobility mac-address** *mac-address* **Example:** `Device(config#) wireless mobility mac-address 000d.bd5e.9f00`	(Optional) Configures the MAC address to be used in mobility messages.
Step 5	**wireless mobility group member ip** *peer-ip* **Example:** `Device(config#) wireless mobility group member ip 9.12.32.15`	Adds a peer in the local group. To remove the peer from the local group, use the **no** form of this command.
Step 6	**wireless mobility dscp** *dscp-value* **Example:** `Device(config#) wireless mobility dscp 52`	(Optional) Configures DSCP. The default value is 48.
Step 7	**wireless mobility group keepalive count** *count* **Example:**	Configures the mobility control and data path keepalive count. The default value is 3.

	Command or Action	Purpose
	`Device(config#) wireless mobility group keepalive count 10`	
Step 8	**wireless mobility group keepalive interval** *interval* **Example:** `Device(config#) wireless mobility group keepalive interval 30`	Configures the mobility control and data path keepalive interval. The default value is 10. **Note** For controllers connected through mobility tunnels, ensure that both controllers have the same keepalive interval value.

Verifying Mobility

To display the summary of the mobility manager, use the following command:

```
Device# show wireless mobility summary
```

To display mobility peer information, use the following command:

```
Device# show wireless mobility peer ip 10.0.0.8
```

To display the list of access points known to the mobility group, use the following command:

```
Device# show wireless mobility ap-list
```

To display statistics for the mobility manager, use the following command:

```
Device# show wireless statistics mobility
Mobility event statistics:
     Joined as
         Local                          : 0
         Foreign                        : 0
         Export foreign                 : 2793
         Export anchor                  : 0
     Delete
         Local                          : 2802
         Remote                         : 0
     Role changes
         Local to anchor                : 0
         Anchor to local                : 0
     Roam stats
         L2 roam count                  : 0
         L3 roam count                  : 0
         Flex client roam count         : 0
         Inter-WNCd roam count          : 0
         Intra-WNCd roam count          : 0
         Remote inter-cntrl roam count : 0
         Remote WebAuth pending roams  : 0
     Anchor Request
         Sent                           : 0
           Grant received               : 0
           Deny received                : 0
         Received                       : 0
           Grant sent                   : 0
           Deny  sent                   : 0
     Handoff Status Received
```

```
            Success                       : 0
            Group mismatch                : 0
            Client unknown                : 0
            Client blacklisted            : 14
            SSID mismatch                 : 0
            Denied                        : 0
        Handoff Status Sent
            Success                       : 0
            Group mismatch                : 0
            Client unknown                : 0
            Client blacklisted            : 0
            SSID mismatch                 : 0
            Denied                        : 0
        Export Anchor
            Request Sent                  : 2812
            Response Received             :
                Ok                        : 2793
                Deny - generic            : 19
                Client blacklisted        : 0
                Client limit reached      : 0
                Profile mismatch          : 0
                Deny - unknown reason     : 0
            Request Received              : 0
            Response Sent                 :
                Ok                        : 0
                Deny - generic            : 0
                Client blacklisted        : 0
                Client limit reached      : 0
                Profile mismatch          : 0
MM mobility event statistics:
        Event data allocs                 : 17083
        Event data frees                  : 17083
        FSM set allocs                    : 2826
        FSM set frees                     : 2816
        Timer allocs                      : 8421
        Timer frees                       : 8421
        Timer starts                      : 14045
        Timer stops                       : 14045
        Invalid events                    : 0
        Internal errors                   : 0
        Delete internal errors            : 0
        Roam internal errors              : 0


MMIF mobility event statistics:
        Event data allocs                 : 17088
        Event data frees                  : 17088
        Invalid events                    : 0
        Event schedule errors             : 0
        MMIF internal errors:
          IPC failure                     : 0
          Database failure                : 0
          Invalid parameters              : 0
          Mobility message decode failure : 0
          FSM failure                     : 0
          Client handoff success          : 0
          Client handoff failure          : 14
          Anchor Deny                     : 0
          Remote delete                   : 0
          Tunnel down delete              : 0
          MBSSID down                     : 0
          Unknown failure                 : 0
```

To display counters for all messages in mobility, use the following command:

```
Device# show wireless stats mobility messages
MM datagram message statistics:
  Message Type               Built  Tx    Rx    Processed  Tx Error  Rx Error  Forwarded
Retry  Drops  Allocs  Frees

--------------------------------------------------------------------------------------------------------------

  Mobile Announce            0      0     0     0          0         0         25350
5624   0      2826    2826
  Mobile Announce Nak        0      0     0     0          0         0         0
0      0      0       0
  Static IP Mobile Annc      0      0     0     0          0         0         0
0      0      0       0
  Static IP Mobile Annc Rsp  0      0     0     0          0         0         0
0      0      0       0
  Handoff                    0      0     14    14         0         0         0
0      0      42      42
  Handoff End                0      0     0     0          0         0         2783
0      0      2783    2783
  Handoff End Ack            0      0     2783  2783       0         0         0
0      0      8349    8349
  Anchor Req                 0      0     0     0          0         0         0
0      0      0       0
  Anchor Grant               0      0     0     0          0         0         0
0      0      0       0
  Anchor Xfer                0      0     0     0          0         0         0
0      0      0       0
  Anchor Xfer Ack            0      0     0     0          0         0         0
0      0      0       0
  Export Anchor Req          0      0     0     0          0         0         2812
0      0      2812    2812
  Export Anchor Rsp          0      0     2812  2812       0         0         0
0      0      8436    8436
  AAA Handoff                0      0     0     0          0         0         0
0      0      0       0
  AAA Handoff Ack            0      0     0     0          0         0         0
0      0      0       0
  IPv4 Addr Update           0      0     2792  0          0         0         0
0      0      2792    2792
  IPv4 Addr Update Ack       2792   2792  0     0          0         0         0
0      0      2792    2792
  IPv6 ND Packet             0      0     0     0          0         0         0
0      0      0       0
  IPv6 Addr Update           0      0     5587  0          0         0         0
0      0      5587    5587
  IPv6 Addr Update Ack       5587   5587  0     0          0         0         0
0      0      5587    5587
  Client Add                 0      0     0     0          0         0         0
0      0      0       0
  Client Delete              0      0     0     0          0         0         0
0      0      0       0
  AP List Update             25585  25585 8512  8512       2         1         0
0      0      34098   34098
  Client Device Profile Info 0      0     0     0          0         0         0
0      0      0       0
  PMK Update                 0      0     0     0          0         0         0
0      0      0       0
  PMK Delete                 0      0     0     0          0         0         0
0      0      0       0
  PMK 11r Nonce Update       0      0     0     0          0         0         0
0      0      0       0
  Device cache Update        0      0     0     0          0         0         0
0      0      0       0
  HA SSO Announce            0      0     0     0          0         0         0
```

```
0       0       0       0
  HA SSO Announce Resp        0       0     0     0          0          0          0
0       0       0       0
  Mesh Roam Request           0       0     0     0          0          0          0
0       0       0       0
  Mesh Roam Response          0       0     0     0          0          0          0
0       0       0       0
  Mesh AP PMK Time Upd        0       0     0     0          0          0          0
0       0       0       0
  Mesh AP PMK Time Upd Ack    0       0     0     0          0          0          0
0       0       0       0
  Mesh AP Channel List        0       3     1     0          0          1          0
0       0       2       2
  Mesh AP Channel List Resp   0       0     0     0          0          0          0
0       0       0       0
  AP upgrade                  0       0     0     0          0          0          0
0       0       0       0
  Keepalive Ctrl Req        34080   34080   17031   17031      0          0          0
0       0       51111   51111
  Keepalive Ctrl Resp       17031   17031   34067   34067      0          0          0
0       0       51098   51098
  Keepalive Data Req/Resp   238527  238527  221451  221451     0          0          0
0       0       459978  459978
```

To display mobility information of the client, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 detail
```

To display roaming history of the active client in the subdomain, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 mobility history
```

To display client-specific statistics for the mobility manager, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 stats mobility
```

To verify whether intercontroller roam is successful, use the following commands:

- **show wireless client mac** *mac-address* **detail**: (on the roamed-to Controller) Displays the roam type as L2 and the roam count is incremented by 1.
- **show wireless client summary** : (on the roamed-from controller) The client entry will not be there in the output.

Verifying SDA Mobility

To verify whether intracontroller, intra-xTR roam is successful, use the following commands:

- **show wireless client summary**: Displays the new AP if the client has roamed across the APs on the same xTR.
- **show wireless client mac** *mac-address* **detail**: Displays the same RLOC as before the roam.

To verify whether intracontroller, inter-xTR roam is successful, use the following commands:

- **show wireless fabric client summary**: Displays the new AP if the client has roamed across the APs on a different xTR.
- **show wireless client mac** *mac-address* **detail**: Displays the RLOC of the new xTR to which the client has roamed to.

To check client status before and after intracontroller roaming, perform the following steps:

1. Check if client is on the old AP, using **show wireless client summary** command on the controller.
2. Check whether the client MAC is listed against the old AP, using **show mac addr dyn** command on the xTR1.
3. Check whether the client IP is registered from current xTR1, and client MAC is registered from both current xTR1, and WLC1, using **show lisp site detail** command on the MAP server.
4. After the intra-WLC roam, check whether the client is on the new AP, using the **show wireless client summary** and **show mac addr dyn** commands on the WLC1 and xTR1.
5. After the Inter-xTR Roam (old and new APs on different xTRs), check whether the client is on the new AP (connected to the new xTR2), using the **show wireless client summary** and **show mac addr dyn** commands on the WLC1 and xTR2.
6. Check whether the client is registered from the new xTR2, using the **show lisp site detail** command on the MAP server.

Verifying Roaming on MAP Server for SDA

To verify roaming information for SDA, use the following commands:

Run the following command on the MAP server, before and after the roam, to check whether the client IP is registered from current xTR, and client MAC is registered from both current xTR, and WLC.

```
Device# show lisp site detail
```

CHAPTER 133

NAT Support on Mobility Groups

- Information About NAT Support on Mobility Groups, on page 1437
- Restrictions for NAT Support on Mobility Groups, on page 1438
- Functionalities Supported on Mobility NAT, on page 1438
- Configuring a Mobility Peer, on page 1439
- Verifying NAT Support on Mobility Groups , on page 1439

Information About NAT Support on Mobility Groups

The Network Address Translation (NAT) on Mobility Groups feature supports the establishment of mobility tunnels between peer controllers when one or both peers are behind a NAT. This is achieved by translating the public and private IP addresses of the peers (see figure below). Depending on the placement and number of NATs, translation might be required at one or both ends of the tunnel.

Figure 45: Mobility NAT



When configuring a NATed mobility peer, both the private IP address (address in the network before the NAT device) and the public IP address (address in the public network) have to be configured. Also, if you are using a firewall, ensure that the ports listed below can be accessed through the firewall:

- Port 16666 for mobility control messages

- Port 16667 for mobility data messages

Restrictions for NAT Support on Mobility Groups

- Only 1:1 (static) NAT entries can exist for the controller peers that form the mobility tunnels.
- Configuring multiple peers with the same public IP address is not supported.
- Private IP addresses of the configured peers must be unique.
- Port Address Translation (PAT) is not supported.
- If peer controllers of different types, for example, Cisco AireOS and Cisco Catalyst 9800 Series) are placed behind NAT, Inter-Release Controller Mobility (IRCM) is not supported for client roaming.
- IPv6 address translation is not supported.

Functionalities Supported on Mobility NAT

The following table lists the functionalities supported on mobility NAT:

Table 99: Functionalities Supported on Mobility NAT

Two controllers, with the foreign controller behind a NAT device (1to1 NAT only)	Yes
Two controllers, with the anchor controller behind a NAT device (1to1 NAT only)	Yes
Two controllers, with the anchor and foreign controller behind a NAT device (1to1 NAT only)	Yes
Multiple foreign and anchor controllers behind NATs (1to1 NAT only)	Yes
Supported Cisco Catalyst 9800 Series Wireless Controllers	• Cisco Catalyst 9800-40 Wireless Controller • Cisco Catalyst 9800-80 Wireless Controller • Catalyst 9800 Wireless Controller for Cloud • Cisco Catalyst 9800-L Wireless Controller
Number of peers supported	72
Manageability using SNMP, Yang, and web UI	Yes
IRCM support for mobility	Yes

SSO	Yes
Client roaming (Layer 2 and Layer 3) between Cisco Catalyst 9800 Series Wireless Controllers	Yes
Client roaming (Layer 2 and Layer 3) between Cisco Catalyst 9800 Series Wireless Controller and AireOS controller	No
Supported applications on the mobility tunnel	• Native profiling • AP list • PMK cache • Mesh AP

Configuring a Mobility Peer

Before you begin

Ensure that the private and public IP addresses of a mobility peer are of the same type, either IPv4 or IPv6.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility group member mac-address** *peer_mac* **ip** *peer_private_ip* [**public-ip** *peer_public_ip*] **group** *group_name* **Example:** `Device(config)# wireless mobility group member mac-address 001e.494b.04ff ip 11.0.0.2 public-ip 4.0.0.112 group dom1`	Adds a mobility peer to the list with an optional public IP address. **Note** You cannot configure multiple peers with the same private or public IP address.
Step 3	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Verifying NAT Support on Mobility Groups

To display the mobility information of a client, use the following command:

```
Device# show wireless client mac-address 000a.bd15.0010 detail
```

```
Client MAC Address : 000a.bd15.0010
Client IPv4 Address : 100.100.0.2
Client Username: N/A
AP MAC Address : 000a.ad00.0800
AP Name: SIM-AP-7
AP slot : 1
.
.
.
```

To display mobility peer information using a private peer IP address, use the following command:

```
Device# show wireless mobility peer ip 21.0.0.2

Mobility Peer Info
==================
Ip Address : 21.0.0.2
Public Ip Address : 3.0.0.22
MAC Address : cc70.ed02.c3b0
Group Name : dom1
.
.
.
```

CHAPTER 134

Static IP Client Mobility

- Information About Static IP Client Mobility, on page 1441
- Restrictions, on page 1441
- Configuring Static IP Client Mobility (GUI), on page 1442
- Configuring Static IP Client Mobility (CLI), on page 1442
- Verifying Static IP Client Mobility, on page 1443

Information About Static IP Client Mobility

At times, you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they might try associating with other controllers.

If the clients try to associate with a controller that does not support the same subnet as the static IP address, the clients fail to connect to the network. The controller inspects the ARP requests sent by the clients to determine if the clients are using static IP addresses or IP addresses that were previously assigned by DHCP. If the ARP requests contain IP addresses that do not exist on any of the controller's Switched Virtual Interfaces (SVIs), the clients are disconnected due to a "VLAN_FAIL" error, resulting in client traffic backhauled without explicit disconnection.

The disconnection due to VLAN mismatch is a change in functionality introduced in the 17.9.1 release.

Static IP clients with static IP addresses can be associated with other controllers in which the client's subnet is supported by tunneling the traffic to another controller in the same mobility group. This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses.

Restrictions

- This feature is not supported on the Fabric and Cisco Catalyst 9800 Wireless Controller for Switch platforms.
- IPv6 is not supported.
- FlexConnect mode is not supported.
- WebAuth (LWA and CWA) is not supported.
- Supported only Open, Dot1x, and PSK authentication mechanisms.

- Supports only on the WLANs that are exclusive of the mobility anchor configuration. If the mobility anchor is already configured on a WLAN, and if static IP mobility is enabled, the feature is not supported.
- Supported only when all the peers are configured for the static IP mobility that is enabled.
- IRCM is not supported.

Configuring Static IP Client Mobility (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy** page, click the policy profile name or click **Add** to create a new one.

Step 3 Click the **Mobility** tab.

Step 4 Set the **Static IP Mobility** field to **Enabled** state.

Step 5 Click **Update & Apply to Device**.

Configuring Static IP Client Mobility (CLI)

Follow the procedure given below to configure static IP client mobility:

Before you begin

- Configure the SVI interface (L3 VLAN interface) to service the static IP client on at least one of the peer controllers in the network.
- For clients to join a controller, the VLAN (based on the VLAN number in the policy profile configuration) should be configured on the device.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy static-ip-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**static-ip-mobility** **Example:**	Enables static IP mobility.

	Command or Action	Purpose
	Device(config-wireless-policy)# static-ip-mobility	

Verifying Static IP Client Mobility

Use the following commands to verify the static IP client mobility configuration:

```
Device# show wireless profile policy detailed static-ip-policy


Policy Profile Name           : static-ip-policy
Description                   :
Status                        : DISABLED
VLAN                          : 1
Wireless management interface VLAN        : 34
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : DISABLED
  Flex NAT PAT            : DISABLED
  Central Assoc               : DISABLED
WLAN Flex Policy
  VLAN based Central Switching           : DISABLED
WLAN ACL
  IPv4 ACL                    : Not Configured
  IPv6 ACL                    : Not Configured
  Layer2 ACL                  : Not Configured
  Preauth urlfilter list      : Not Configured
  Postauth urlfilter list     : Not Configured
WLAN Timeout
  Session Timeout             : 1800
  Idle Timeout                : 300
  Idle Threshold              : 0
WLAN Local Profiling
  Subscriber Policy Name      : Not Configured
  RADIUS Profiling            : DISABLED
  HTTP TLV caching            : DISABLED
  DHCP TLV caching            : DISABLED
WLAN Mobility
  Anchor                      : DISABLED
AVC VISIBILITY                : Disabled
Flow Monitor IPv4
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
Flow Monitor IPv6
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
NBAR Protocol Discovery       : Disabled
Reanchoring                   : Disabled
Classmap name for Reanchoring
  Reanchoring Classmap Name   : Not Configured
QOS per SSID
  Ingress Service Name        : Not Configured
  Egress Service Name         : Not Configured
QOS per Client
  Ingress Service Name        : Not Configured
```

```
  Egress Service Name         : Not Configured
Umbrella information
  Cisco Umbrella Parameter Map : Not Configured
Autoqos Mode                  : None
Call Snooping                 : Disabled
Fabric Profile
  Profile Name                : Not Configured
Accounting list
  Accounting List               : Not Configured
DHCP
  required                    : DISABLED
  server address              : 0.0.0.0
 Opt82
  DhcpOpt82Enable             : DISABLED
  DhcpOpt82Ascii              : DISABLED
  DhcpOpt82Rid                : DISABLED
  APMAC                       : DISABLED
  SSID                        : DISABLED
  AP_ETHMAC                   : DISABLED
  APNAME                      : DISABLED
  POLICY TAG                  : DISABLED
  AP_LOCATION                 : DISABLED
  VLAN_ID                     : DISABLED
Exclusionlist Params
  Exclusionlist               : ENABLED
  Exclusion Timeout           : 60
AAA Policy Params
  AAA Override                : DISABLED
  NAC                         : DISABLED
  AAA Policy name             : default-aaa-policy
WGB Policy Params
  Broadcast Tagging           : DISABLED
  Client VLAN                 : DISABLED
Mobility Anchor List
  IP Address                                  Priority
  -------------------------------------------------------
```

```
Device# show run | section profile policy

wireless profile policy default-policy-profile
 central switching
 description "default policy profile"
 static-ip-mobility
 vlan 50
 no shutdown
```

CHAPTER 135

Mobility Domain ID - Dot11i Roaming

- Information about Mobility Domain ID - 802.11i Roaming, on page 1445
- Verifying Mobility Domain ID - 802.11i Roaming, on page 1446

Information about Mobility Domain ID - 802.11i Roaming

A mobility domain is a cluster of APs forming a continuous radio frequency space, where the Pairwise Master Key (PMK) can be synchronized, and fast roaming can be enabled for 802.11r (Fast Transition) or 802.11i (WPA).

In the releases prior to Cisco IOS XE 17.2.1, the PMK cache was shared across the FlexConnect APs using the AP site tag. All the APs that are a part of a site tag share the PMK cache. This is applicable only for central authentication.

From Cisco IOS XE 17.2.1, you can create a Mobility Domain ID (MDID) for each of the APs. All the APs with the same MDID share the PMK cache keys even if they are in different site tags. When MDID is configured for APs, the PMK cache keys are not shared with the APs that are not a part of the same MDID, even if they are a part of the same site tag. MDID supports PMK cache distribution for both central authentication and local authentication.

Note

- The Mobility Domain ID - 802.11i Roaming feature does not work when the Flex APs are in standalone mode because the feature depends on the controller to share the keys.
- MDID is configured only through the open configuration model. There is no CLI or GUI support.
- In Cisco IOS XE Amsterdam 17.2.1, 100 APs per site-tag or per MDID are supported, and 1000 PMK entries are supported per AP.

The mobility domain can either be defined as a static configuration of clustered APs, all under a commonly configured MDID, or dynamically computed. You can implement a spatial clustering algorithm based on neighbor associations of APs. Each AP can only be a part of one roaming domain.

An MDID is used by 802.11r to define a network in which an 802.11r fast roam is supported. PMKs should be shared within mobility domains, allowing clients to support fast roaming. If defined, MDID takes precedence over a site tag.

MDID configurations are exercised only from open configuration models. For more information about open configuration models, see the https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/172/b_172_programmability_cg.html.

Verifying Mobility Domain ID - 802.11i Roaming

The following examples shows how to view and verify the 802.11i Roaming configuration:

```
Device#  show running-config | section specific-config
ap specific-config 58ac.70dc.xxxx hostname AP58AC.70DC.XXXX
   roaming-domain roaming_domain_2
ap specific-config 78xc.f09d.xxxx hostname AP78XC.F09D.XXXX
   roaming-domain roaming_domain_3
```

CHAPTER 136

802.11r Support for Flex Local Authentication

- Information About 802.11r Support for FlexConnect Local Authentication, on page 1447
- Verifying 802.11r Support for Flex Local Authentication , on page 1448

Information About 802.11r Support for FlexConnect Local Authentication

In releases prior to Cisco IOS XE Amsterdam 17.2.1, the FlexConnect mode fast transition was supported only in centrally authenticated clients. This was achieved by sharing the Pairwise Master Key (PMK) to all the FlexConnect APs in the same site tag. From Cisco IOS XE Amsterdam 17.2.1, fast transition is supported even for locally authenticated clients.

The client PMK cache entries are shared and distributed to all the APs in the same site tag. From Cisco IOS XE Amsterdam 17.2.1, another grouping called Mobility Domain ID (MDID) is introduced, for sharing the PMK cache entries. MDID can be configured for APs using the open configuration model only. There is no CLI or GUI support.

The PMK cache distribution in a FlexConnect local site (using either the site tag or MDID) is restricted to 100 APs per group, with a maximum support for 1000 PMK entries per AP.

Support Guidelines

The following are the 802.11r support guidelines:

- Supports 802.11r on FlexConnect local authentication only with Over-the-Air method of roaming. Over-the-DS (Distribution System) is not supported.
- Supports adaptive 11r for Apple clients.
- Supports both Fast Transition + 802.1x and Fast Transition + PSK.

Note This is supported only when clients join the standalone mode AP.

Verifying 802.11r Support for Flex Local Authentication

To verify the number of PMK caches, use the **show wireless pmk-cache** command:

```
Device# show wireless pmk-cache
Number of PMK caches in total : 1

Type      Station            Entry Lifetime  VLAN Override         IP Override
Audit-Session-Id             Username
------------------------------------------------------------------------------
DOT11R    74xx.bx5a.07xx     87              NA
000000000000000FF3562B5D     jey
```

To verify the 802.11r flex roam attempts, use the **show wireless client mac-address 74xx.bx5a.07xx mobility history** command:

```
Device# show wireless client mac-address 74xx.bx5a.07xx mobility history
Recent association history (most recent on top):

AP Name                                     BSSID           AP Slot    Assoc Time
        Instance   Mobility Role   Run Latency (ms)     Dot11 Roam Type


------------------------------------------------------------------------------------------------------------


APM-9120-1-GCP                              d4xx.80xx.8fxx  1          12/11/2019 18:44:37
      1          Local           2                    802.11R


APM-4800-3                                  f4xx.e6xx.08xx  1          12/11/2019 18:43:02
      1          Local           17547                N/A

show wireless stats client detail | sec roam
Total 11r flex roam attempts                    : 1
```

CHAPTER 137

Opportunistic Key Caching

- Information about Opportunistic Key Caching, on page 1449
- Enabling Opportunistic Key Caching, on page 1450
- Enabling Opportunistic Key Caching (GUI), on page 1450
- Verifying Opportunistic Key Caching, on page 1450

Information about Opportunistic Key Caching

Opportunistic Key Caching (OKC) is an enhancement of the WPA2 Pairwise Master Key ID (PMKID) caching method, which is why it is also named Proactive or Opportunistic PMKID Caching. Just like PMKID caching, OKC works with WPA2-EAP.

The OKC technique allows wireless clients and the WLAN infrastructure to cache only one PMK for client association with a WLAN, even when roaming between multiple APs because they all share the original PMK that is used for the WPA2 4-way handshake. This is required to generate new encryption keys every time a client reassociates with APs. For APs to share the original PMK from a client session, they must all be under a centralized device that caches and distributes the original PMK to all the APs.

Just as in PMKID caching, the initial association to an AP is a regular first-time authentication to the corresponding WLAN, where you must complete the entire 802.1X/EAP authentication for the authentication server, and the 4-way handshake for key generation, before sending data frames.

OKC is a fast roaming technique supported by Microsoft and some Android clients. Another fast roaming method is the use of 802.11r, which is supported by Apple and few Android clients. OKC is enabled by default on a WLAN. This configuration enables the control of OKC on a WLAN. Disabling OKC on a WLAN disables the OKC even for the OKC-supported clients.

A new configuration is introduced for each WLAN in the controller in Cisco IOS XE Amsterdam 17.2.1, to disable or enable fast and secure roaming with OKC at the corresponding AP.

Enabling Opportunistic Key Caching

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-identifier <1-4096> ssid-network-name* **Example:** `Device(config)# wlan wlan-profile-name 18 san-ssid`	Enters WLAN configuration submode. *wlan-profile-name*: Profile name of the configured WLAN.
Step 3	**okc** **Example:** `Device(config-wlan)# okc`	Enables Opportunistic Key Caching, if not enabled. By default, the OKC feature is enabled. (Use the **no** form of this command to disable the OKC feature.)

Enabling Opportunistic Key Caching (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

The **Add WLAN** dialog box is displayed.

Step 3 In the **Add WLAN** dialog box, click the **Advanced** tab and complete the following procedure:

a) In the **11ax** section, check the **OKC** check box to disable or enable the feature. By default this feature is enabled.

b) Click **Update & Apply to Device**.

Verifying Opportunistic Key Caching

The following example shows how to verify whether OKC is disabled for a WLAN profile.

- `Device# show wlan id 18`

```
WLAN Profile Name     : 18%wlanprofile
=================================================
Identifier                                 : 18
```

```
Description                                     :
Network Name (SSID)                             : san-ssid
Status                                          : Disabled
Broadcast SSID                                  : Enabled
Advertise-Apname                                : Disabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
OKC                                             : Disabled
Number of Active Clients                        : 0
CHD per WLAN                                    : Enabled
WMM                                             : Allowed
Channel Scan Defer Priority:
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Disabled
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
```

- Device# **show run wlan**

```
wlan name 2 ssid-name
wlan test 24 test
wlan test2 15 test2
wlan test4 12 testssid
 radio dot11a
wlan wlan1 234 wlan1
wlan wlan2 14 wlan-aaa
 security dot1x authentication-list realm
wlan wlan7 27 wlan7
wlan test23 17 test23
wlan wlan_1 4 ssid_name
 security dot1x authentication-list authenticate_list_name
wlan wlan_3 5 ssid_3
 security wpa wpa1
 security wpa wpa1 ciphers aes
wlan wlan_8 9 ssid_name
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 security web-auth
wlan test-wlan 23 test-wlan
wlan wlan-test 1 wlan2
 mac-filtering default
wlan 18%wlanprofile 18 san-ssid
 no okc
```

PART IX

High Availability

- High Availability, on page 1455

CHAPTER 138

High Availability

- Feature History for High Availability, on page 1456
- Information About High Availability, on page 1457
- Prerequisites for High Availability, on page 1458
- Restrictions on High Availability, on page 1459
- Configuring High Availability (CLI), on page 1460
- Disabling High Availability, on page 1461
- Copying a WebAuth Tar Bundle to the Standby Controller, on page 1462
- System and Network Fault Handling, on page 1464
- Handling Recovery Mechanism, on page 1469
- Verifying High Availability Configurations, on page 1470
- Verifying AP or Client SSO Statistics, on page 1470
- Verifying High Availability, on page 1472
- High Availability Deployment for Application Centric Infrastructure (ACI) Network, on page 1475
- Configuring a Switchover, on page 1479
- Information About Redundancy Management Interface, on page 1479
- Configuring Redundancy Management Interface (GUI), on page 1484
- Configuring Redundancy Management Interface (CLI), on page 1485
- Configuring Gateway Monitoring (CLI), on page 1487
- Configuring Gateway Monitoring Interval (CLI), on page 1487
- Gateway Reachability Detection, on page 1488
- Monitoring the Health of the Standby Controller, on page 1489
- Monitoring the Health of Standby Parameters Using SNMP, on page 1491
- Monitoring the Health of Standby Controller Using Programmatic Interfaces, on page 1493
- Monitoring the Health of Standby Controller Using CLI, on page 1493
- Verifying the Gateway-Monitoring Configuration, on page 1497
- Verifying the RMI IPv4 Configuration, on page 1497
- Verifying the RMI IPv6 Configuration, on page 1499
- Verifying Redundancy Port Interface Configuration, on page 1499
- Information About Auto-Upgrade, on page 1502
- Configuration Workflow, on page 1502
- Configuring Auto-Upgrade (CLI), on page 1503
- Use Case for Link Layer Discovery Protocol (LLDP), on page 1503
- Enabling LLDP (CLI), on page 1503

• Enabling LLDP Timers (CLI), on page 1504
• Enabling LLDP TLV-Select (CLI), on page 1504
• Verifying LLDP, on page 1505

Feature History for High Availability

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 100: Feature History for High Availability

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.1.1s	Redundant Management Interface	The Redundancy Management Interface (RMI) is used as a secondary link between the active and standby controllers. This interface is the same as the Wireless Management Interface and the IP address on this interface is configured in the same subnet as the Wireless Management Interface.
Cisco IOS XE Bengaluru 17.4.1	Gateway Reachability Detection	Gateway reachability feature minimizes the downtime on APs and clients when the gateway reachability is lost on the active controller.
Cisco IOS XE Bengaluru 17.5.1	Standby Monitoring Enhancements	The Standby Monitoring Enhancements feature monitors the standby CPU or memory information from the active controller. Also, this feature independently monitors the standby controller using SNMP for the interface MIB. The cLHaPeerHotStandbyEvent and cLHaPeerHotStandbyEvent MIB objects in CISCO-HA-MIB are used to monitor the standby HA status.
Cisco IOS XE Bengaluru 17.5.1	Auto-Upgrade	The auto-upgrade feature enables the standby controller to upgrade to active controller's software image, so that both controllers can form an high availability (HA) pair.
Cisco IOS XE Bengaluru 17.6.1	Standby Interface Status using Active SNMP	This feature allows the standby controller interface status to be queried at the active using SNMP.

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	High Availability Deployment for Application Centric Infrastructure (ACI) Network	This feature avoids interleaving traffic between the old and new active controller using the following functionalities: • Bringing down Wireless Management Interface (WMI) faster. • Disabling fast switchover notification.
	Link Layer Discovery Protocol (LLDP) Support in the Standby Controller	From this release, the Link Layer Discovery Protocol (LLDP) process will be up and running in both active and standby controllers.

Information About High Availability

High Availability (HA) allows you to reduce the downtime of wireless networks that occurs due to the failover of controllers. The HA Stateful Switch Over (SSO) capability on the controller allows AP to establish a CAPWAP tunnel with the active controller. The active controller shares a mirror copy of the AP and client database with the standby controller. The APs won't go into the discovery state and clients don't disconnect when the active controller fails. The standby controller takes over the network as the active controller. Only one CAPWAP tunnel is maintained between the APs and the controller that is in an active state.

HA supports full AP and client SSO. Client SSO is supported only for clients that have completed the authentication and DHCP phase, and have started passing traffic. With Client SSO, the client information is synced to the standby controller when the client associates to the controller or when the client parameters change. Fully authenticated clients, for example, the ones in RUN state, are synced to the standby. Thus, client reassociation is avoided on switchover making the failover seamless for the APs and clients, resulting in zero client service downtime and zero SSID outage. This feature reduces major downtime in wireless networks due to failure conditions such as box failover, network failover, or power outage on the primary site.

Note

- In HA mode, the RP port shut or no shut should not be performed during the controller bootup.
- If the RP communication is lost between active and standby controller during HA sync, the standby controller crashes as the IPC communication fails. The crash is intentional.

  If RP link is restored, the standby controller gracefully reloads and forms an HA pair.

Note When the controller works as a host for spanning tree, ensure that you configure portfast trunk, using **spanning-tree port type edge trunk** or **spanning-tree portfast trunk** commands, in the uplink switch to ensure faster convergence.

Note You can configure FIPS in HA setup. For information, see the Configuring FIPS in HA Setup.

Note The IPv4 secondary address is used internally for RMI purpose. So, it is not recommended to configure the secondary IPv4 address.

In case of IPv6, only one management IPv6 is allowed, secondary address is configured for RMI-IPv6 purpose. It is not recommended to have more than one IPv6 management on the Wireless Management Interface (WMI).

More than one management IPv4 and IPv6 addresses on WMI can result in unpredictable behavior.

Prerequisites for High Availability

External Interfaces and IPs

Because all the interfaces are configured only on the Active box, but are synchronized with the Standby box, the same set of interfaces are configured on both controllers. From external nodes, the interfaces connect to the same IP addresses, irrespective of the controllers they are connected to.

For this purpose, the APs, clients, DHCP, Cisco Prime Infrastructure, Cisco Catalyst Centre, and Cisco Identity Services Engine (ISE) servers, and other controller members in the mobility group always connect to the same IP address. The SSO switchover is transparent to them. But if there are TCP connections from external nodes to the controller, the TCP connections need to be reset and reestablished.

HA Interfaces

The HA interface serves the following purposes:

- Provides connectivity between the controller pair before an IOSd comes up.
- Provides IPC transport across the controller pair.
- Enables redundancy across control messages exchanged between the controller pair. The control messages can be HA role resolution, keepalives, notifications, HA statistics, and so on.

You can select either SFP or RJ-45 connection for HA port. Supported Cisco SFPs are:

- GLC-SX-MMD
- GLC-LH-SMD

When either SFP or RJ-45 connection is present, HA works between the two controllers. The SFP HA connectivity takes priority over RJ-45 HA connectivity. If SFP is connected when RJ-45 HA is up and running, the HA pair reloads. The reload occurs even if the link between the SFPs isn't connected.

Note

- It is recommended to have a dedicated physical NIC and Switch for RP when the HA pair is deployed across two host machines. This avoids any keep-alive loses and false HA switchovers or alarms.
- Disable security scans on VMware virtual instances.

Restrictions on High Availability

- For a fail-safe SSO, wait till you receive the switchover event after completing configuration synchronization on the standby controller. If the standby controller has just been booted up, we recommend that you wait *x* minutes before the controller can handle switchover events without any problem. The value of *x* can change based on the platform. For example, a Cisco 9800-80 Series Controller running to its maximum capacity can take up to 24 minutes to complete the configuration synchronization before being ready for SSO. You can use the **show wireless stats redundancy config database** command to view the database-related statistics.
- The flow states of the NBAR engine are lost during a switchover in an HA scenario in local mode. Because of this, the classification of flows will restart, leading to incorrect packet classification as the first packet of the flow is missed.
- The HA connection supports only IPv4.
- Switchover and an active reload and forces a high availability link down from the new primary.
- Hyper threading is not supported and if enabled HA keepalives will be lost in case of an HA system that results in stack merge.
- Standby RMI interface does not support Web UI access.
- Two HA interfaces (RMI and RP) must be configured on the same subnet, and the subnet cannot be shared with any other interfaces on the device.
- It is not possible to synchronize a TCP session state because a TCP session cannot survive after a switchover, and needs to be reestablished.
- The Client SSO does not address clients that have not reached the RUN state because they are removed after a switchover.
- Statistics tables are not synced from active to standby controller.
- Machine snapshot of a VM hosting controller HA interfaces is not supported. It may lead to a crash in the HA controller.
- Mobility-side restriction: Clients which are not in RUN state will be forcefully reauthenticated after switchover.
- The following application classification may not be retained after the SSO:
    - AVC limitation—After a switchover, the context transfer or synchronization to the Standby box does not occur and the new active flow needs to be relearned. The AVC QoS does not take effect during classification failure.
    - A voice call cannot be recognized after a switchover because a voice policy is based on RTP or RTCP protocol.
    - Auto QoS is not effective because of AVC limitation.
- The active controller and the standby controller must be paired with the same interface for virtual platforms. For hardware appliance, there is a dedicated HA port.
- Static IP addressing can synch to standby, but the IP address cannot be used from the standby controller.

- You can map a dedicated HA port to a 1 GB interface only.
- To use EtherChannels in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x, ensure that the channel mode is set to On.
- EtherChannel Auto-mode is not supported in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x.
- LACP and PAGP is not supported in HA mode in releases until, and including, Cisco IOS XE Gibraltar 16.12.x.
- When the controller works as a host for spanning tree, ensure that you configure portfast trunk in the uplink switch using s**panning-tree port type edge trunk** or **spanning-tree portfast trunk** command to ensure faster convergence.
- The **clear chassis redundancy** and **write erase** commands will not reset the chassis priority to the default value.
- While configuring devices in HA, the members must not have wireless trustpoint with the same name and different keys. In such a scenario, if you form an HA pair between the two standalone controllers, the wireless trustpoint does not come up after a subsequent SSO. The reason being the *rsa keypair* file exists but it is incorrect as the *nvram:private-config* file is not synched with the actual *WLC_WLC_TP* key pair.

  As a best practice, before forming an HA, it is recommended to delete the existing certificates and keys in each of the controllers which were previously deployed as standalone.
- After a switchover, when the recovery is in progress, do not configure the WLAN or WLAN policy. In case you configure, the controller can crash.
- After a switchover, clients that are not in RUN state and not connected to an AP are deleted after 300 seconds.

Configuring High Availability (CLI)

Before you begin

The active and standby controller should be in the same mode, either Install mode or Bundle mode, with same image version. We recommend that you use Install mode.

Procedure

	Command or Action	Purpose
Step 1	**chassis** *chassis-num* **priority** *chassis-priority* **Example:** `Device# chassis 1 priority 1`	(Optional) Configures the priority of the specified device. **Note** From Cisco IOS XE Gibraltar 16.12.x onwards, device reload is not required for the chassis priority to become effective.

	Command or Action	Purpose
		• *chassis-num*—Enter the chassis number. The range is from 1 to 2. • *chassis-priority*—Enter the chassis priority. The range is from 1 to 2. The default value is 1. **Note** When both the devices boot up at the same time, the device with higher priority(2) becomes active, and the other one becomes standby. If both the devices are configured with the same priority value, the one with the smaller MAC address acts as active and its peer acts as standby.
Step 2	**chassis redundancy ha-interface GigabitEthernet** *num***local-ip** *local-chassis-ip-addr network-mask* **remote-ip** *remote-chassis-ip-addr* **Example:** `Device# chassis redundancy ha-interface GigabitEthernet 2 local-ip 4.4.4.1 /24 remote-ip 4.4.4.2`	Configures the chassis high availability parameters. • *num*—GigabitEthernet interface number. The range is from 0 to 32. • *local-chassis-ip-addr*—Enter the IP address of the local chassis HA interface. • *network-mask*—Enter the network mask or prefix length in the */nn* or *A.B.C.D* format. • *remote-chassis-ip-addr*—Enter the remote chassis IP address.
Step 3	**chassis redundancy keep-alive timer** *timer* **Example:** `Device# chassis redundancy keep-alive timer 6`	Configures the peer keepalive timeout value. Time interval is set in multiple of 100 ms (enter 1 for default).
Step 4	**chassis redundancy keep-alive retries** *retry-value* **Example:** `Device# chassis redundancy keep-alive retries 8`	Configures the peer keepalive retry value before claiming peer is down. Default value is 5.

Disabling High Availability

If the controller is configured using RP method of SSO configuration, use the following command to clear all the HA-related parameters, such as local IP, remote IP, HA interface, mask, timeout, and priority:

clear chassis redundancy

If the controller is configured using RMI method, use the following command:

no redun-management interface vlan chassis

Note Reload the devices for the changes to take effect.

After the HA unpairing, the standby controller startup configuration and the HA configuration will be cleared and standby will go to Day 0.

Before the command is executed, the user is prompted with the following warning on the active controller:

```
Device# clear chassis redundancy

WARNING: Clearing the chassis HA configuration will result in both the chassis move into
Stand Alone mode. This involves reloading the standby chassis after clearing its HA
configuration and startup configuration which results in standby chassis coming up as a
totally
clean after reboot. Do you wish to continue? [y/n]? [yes]:

*Apr 3 23:42:22.985: received clear chassis.. ha_supported:1yes
WLC#
*Apr 3 23:42:25.042: clearing peer startup config
*Apr 3 23:42:25.042: chkpt send: sent msg type 2 to peer..
*Apr 3 23:42:25.043: chkpt send: sent msg type 1 to peer..
*Apr 3 23:42:25.043: Clearing HA configurations
*Apr 3 23:42:26.183: Successfully sent Set chassis mode msg for chassis 1.chasfs file updated
*Apr 3 23:42:26.359: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected chassis 2 is no
longer standby
```

On the standby controller, the following messages indicate that the configuration is being cleared:

```
Device-stby#

*Apr 3 23:40:40.537: mcprp_handle_spa_oir_tsm_event: subslot 0/0 event=2
*Apr 3 23:40:40.537: spa_oir_tsm subslot 0/0 TSM: during state ready, got event 3(ready)
*Apr 3 23:40:40.537: @@@ spa_oir_tsm subslot 0/0 TSM: ready -> ready
*Apr 3 23:42:25.041: Removing the startup config file on standby

!Standby controller is reloaded after clearing the chassis.
```

Copying a WebAuth Tar Bundle to the Standby Controller

Use the following procedure to copy a WebAuth tar bundle to the standby controller, in a high-availability configuration.

Procedure

Step 1 Choose **Administration > Management > Backup & Restore**.

Step 2 From the **Copy** drop-down list, choose **To Device**.

Step 3 From the **File Type** drop-down list, choose **WebAuth Bundle**.

Step 4 From the **Transfer Mode** drop-down list, choose **TFTP**, **SFTP**, **FTP**, or **HTTP**.

The **Server Details** options change based on the file transfer option selected.

- **TFTP**
  - **IP Address (IPv4/IPv6)**: Enter the server IP address (IPv4 or IPv6) of the TFTP server that you want to use.
  - **File Path**: Enter the file path. The file path should start with slash a (/*path*).
  - **File Name**: Enter a file name.

    The file name should not contain spaces. Underscores (_) and hyphen (-) are the only special characters that are supported. Ensure that file name ends with .tar, for example, webauthbundle.tar.

- **SFTP**
  - **IP Address (IPv4/IPv6)**: Enter the server IP address (IPv4 or IPv6) of the SFTP server that you want to use.
  - **File Path**: Enter the file path. The file path should start with slash a (/*path*).
  - **File Name**: Enter a file name.

    The file name should not contain spaces. Underscores (_) and hyphen (-) are the only special characters that are supported. Ensure that file name ends with .tar, for example, webauthbundle.tar.
  - **Server Login UserName**: Enter the SFTP server login user name.
  - **Server Login Password**: Enter the SFTP server login passphrase.

- **FTP**
  - **IP Address (IPv4/IPv6)**: Enter the server IP address (IPv4 or IPv6) of the TFTP server that you want to use.
  - **File Path**: Enter the file path. The file path should start with slash a (/*path*).
  - **File Name**: Enter a file name.

    The file name should not contain spaces. Underscores (_) and hyphen (-) are the only special characters that are supported. Ensure that file name ends with .tar, for example, webauthbundle.tar.
  - **Logon Type**: Choose the login type as either **Anonymous** or **Authenticated**. If you choose **Authenticated**, the following fields are activated:
    - **Server Login UserName**: Enter the FTP server login user name.
    - **Server Login Password**: Enter the FTP server login passphrase.

- **HTTP**
  - **Source File Path**: Click **Select File** to select the configuration file, and click **Open**.

Step 5 Click the **Yes** or **No** radio button to back up the existing startup configuration to Flash.

Save the configuration to Flash to propagate the WebAuth bundle to other members, including the standby controller. If you do not save the configuration to Flash, the WebAuth bundle will not be propagated to other members, including the standby controller.

Step 6 Click **Download File**.

System and Network Fault Handling

If the standby controller crashes, it reboots and comes up as the standby controller. Bulk sync follows causing the standby to become hot. If the active controller crashes, the standby becomes active. The new active controller assumes the role of primary and tries to detect a dual active.

The following matrices provide a clear picture of the conditions the controller switchover would trigger:

Table 101: System and Network Fault Handling

System Issues				
Trigger	**RP Link Status**	**Peer Reachability through RMI**	**Switchover**	**Result**
Critical process crash	Up	Reachable	Yes	Switchover happens
Forced switchover	Up	Reachable	Yes	Switchover happens
Critical process crash	Up	Unreachable	Yes	Switchover happens
Forced switchover	Up	Unreachable	Yes	Switchover happens
Critical process crash	Down	Reachable	No	No action. One controller in recovery mode.
Forced switchover	Down	Reachable	N/A	No action. One controller in recovery mode.
Critical process crash	Down	Unreachable	No	Double fault – as mentioned in Network Error handling
Forced switchover	Down	Unreachable	N/A	Double fault – as mentioned in Network Error handling

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Up	Reachable	Reachable	Reachable	No SSO	No action
Up	Reachable	Reachable	Unreachable	No SSO	No action. Standby is not ready for SSO in this state, as it does not have gateway reachability. The standby is shown to be in standby-recovery mode. If the RP goes down, standby (in recovery mode) becomes active.
Up	Reachable	Unreachable	Reachable	SSO	Gateway reachability message is exchanged over the RMI + RP links. Active reboots so that the standby becomes active.
Up	Reachable	Unreachable	Unreachable	No SSO	With this, when the active SVI goes down, the standby SVI also goes down. A switchover is then triggered. If the new active discovers its gateway to be reachable, the system stabilizes in the Active - Standby Recovery mode. Otherwise, switchovers happen in a ping-pong fashion.

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Up	Unreachable	Reachable	Reachable	No SSO	No action
Up	Unreachable	Reachable	Unreachable	No SSO	Standby is not ready for SSO in this state as it does not have gateway reachability. Standby moves in to recovery mode as LMP messages are exchanged over the RP link.
Up	Unreachable	Unreachable	Reachable	SSO	Gateway reachability message is exchanged over RP link. Active reboots so that standby becomes active.
Up	Unreachable	Unreachable	Unreachable	No SSO	With this, when the active SVI goes down, the standby SVI also goes down. A switchover is then triggered. If the new active discovers its gateway to be reachable, the system stabilizes in Active - Standby Recovery mode. Otherwise, switchovers happen in a ping-pong fashion.

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Down	Reachable	Reachable	Reachable	No SSO	Standby detects the presence of the Active over the RMI link and avoids switchover when the RP link goes down. In such a case, the standby goes to recovery mode. This mode is represented through suffix **rp-rec-mode** in the hostname. The standby in recovery mode reloads when the RP link comes up. Single faults are gracefully handled in the system.
Down	Reachable	Reachable	Unreachable	No SSO	Same as above.

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Down	Reachable	Unreachable	Reachable	RP link down, then active loses GW, then there won't be any SSO. GW down, within 8 seconds, RP link goes down, then there would be a SSO.	Gateway reachability message is exchanged over RP+RMI links. Old-Active goes to active-recovery mode. The configuration mode is disabled in active-recovery mode. All interfaces will be ADMIN DOWN with the wireless management interface having RMI IP. The controller in active-recovery will reload to become standby (or standby-recovery if gateway reachability is still not available) when the RP link comes up.
Down	Reachable	Unreachable	Unreachable	No SSO	Standby goes to standby-recovery.

RP Link	Peer Reachability Through RMI	Gateway From Active	Gateway From Standby	Switchover	Result
Down	Unreachable	Reachable	Reachable	SSO	Double fault – this may result in a network conflict as there will be two active controllers. Standby becomes active. Old active also exists. Role negotiation has to happen once the connectivity is restored and keep the active that came up last.
Down	Unreachable	Reachable	Unreachable	SSO	Same as above.
Down	Unreachable	Unreachable	Reachable	SSO	Same as above.
Down	Unreachable	Unreachable	Unreachable	SSO	Same as above.

Handling Recovery Mechanism

Active to Active Recovery

- When RP is down and RMI is up at boot up, the Active Recovery occurs.
- When HA is stable (active - standby), if RMI is down first and then RP goes down next, and later if RMI comes up before RP comes up, the Active to Active Recovery occurs. Once the RP is up, the Active Recovery reloads and HA is formed.

Standby to Standby Recovery

- When Standby goes to Standby Recovery for Gateway alone, once the Gateway is up, the HA comes up without any reboot.
- When Standby goes to Standby Recovery for RP down, once the RP is up, the standby recovery reboots automatically and HA is formed.

Verifying High Availability Configurations

To view the HA configuration details, use the following command:

```
Device# show romvar
ROMMON variables:
 LICENSE_BOOT_LEVEL =
 MCP_STARTUP_TRACEFLAGS = 00000000:00000000
 BOOTLDR =
 CRASHINFO = bootflash:crashinfo_RP_00_00_20180202-034353-UTC
 STACK_1_1 = 0_0
 CONFIG_FILE =
 BOOT =
bootflash:boot_image_test,1;bootflash:boot_image_good,1;bootflash:rp_super_universalk9.vwlc.bin,1;

 RET_2_RTS =
 SWITCH_NUMBER = 1
 CHASSIS_HA_REMOTE_IP = 10.0.1.9
 CHASSIS_HA_LOCAL_IP = 10.0.1.10
 CHASSIS_HA_LOCAL_MASK = 255.255.255.0
 CHASSIS_HA_IFNAME = GigabitEthernet2
 CHASSIS_HA_IFMAC = 00:0C:29:C9:12:0B
 RET_2_RCALTS =
 BSI = 0
 RANDOM_NUM = 647419395
```

Verifying AP or Client SSO Statistics

To view the AP SSO statistics, use the following command:

```
Device# show wireless stat redundancy statistics ap-recovery wnc all
AP SSO Statistics

Inst    Timestamp     Dura(ms)   #APs  #Succ  #Fail  Avg(ms)  Min(ms)  Max(ms)
-------------------------------------------------------------------------------
   0    00:06:29.042        98     34     34      0        2        1       35
   1    00:06:29.057        56     33     30      3        1        1       15
   2    00:06:29.070        82     33     33      0        2        1       13


Statistics:

WNCD Instance   : 0
No. of AP radio recovery failures          : 0
No. of AP BSSID recovery failures          : 0
No. of CAPWAP recovery failures            : 0
No. of DTLS recovery failures              : 0
No. of reconcile message send failed       : 0
No. of reconcile message successfully sent : 34
No. of Mesh BSSID recovery failures: 0
No. of Partial delete cleanup done : 0
.
.
.
```

To view the Client SSO statistics, use the following command:

```
Device# show wireless stat redundancy client-recovery wncd all
Client SSO statistics
---------------------
```

```
WNCD instance  : 1
Reconcile messages received from AP                     : 1
Reconcile clients received from AP                      : 1
Recreate attempted post switchover                      : 1
Recreate attempted by SANET Lib                         : 0
Recreate attempted by DOT1x Lib                         : 0
Recreate attempted by SISF Lib                          : 0
Recreate attempted by SVC CO Lib                        : 1
Recreate attempted by Unknown Lib                       : 0
Recreate succeeded post switchover                      : 1
Recreate Failed post switchover                         : 0
Stale client entries purged post switchover             : 0

Partial delete during heap recreate                     : 0
Partial delete during force purge                       : 0
Partial delete post restart                             : 0
Partial delete due to AP recovery failure               : 0
Partial delete during reconcilation                     : 0

Client entries in shadow list during SSO                : 0
Client entries in shadow default state during SSO       : 0
Client entries in poison list during SSO                : 0

Invalid bssid during heap recreate                      : 0
Invalid bssid during force purge                        : 0
BSSID mismatch with shadow rec during reconcilation     : 0
BSSID mismatch with shadow rec reconcilation(WGB client): 0
BSSID mismatch with dot11 rec during heap recreate      : 0

AID mismatch with dot11 rec during force purge          : 0
AP slotid mismatch during reconcilation                 : 0
Zero aid during heap recreate                           : 0
AID mismatch with shadow rec during reconcilation       : 0
AP slotid mismatch shadow rec during reconcilation      : 0
Client shadow record not present                        : 0
```

To view the mobility details, use the following command:

```
Device# show wireless stat redundancy client-recovery mobilityd
Mobility Client Deletion Reason Statistics
------------------------------------------
Mobility Incomplete State         : 0
Inconsistency in WNCD & Mobility  : 0
Partial Delete                    : 0

General statistics
--------------------
Cleanup sent to WNCD, Missing Delete case   : 0
```

To view the Client SSO statistics for SISF, use the following command:

```
Device# show wireless stat redundancy client-recovery sisf
Client SSO statistics for SISF
------------------------------
Number of recreate attempted post switchover    : 1
Number of recreate succeeded post switchover    : 1
Number of recreate failed because of no mac     : 0
Number of recreate failed because of no ip      : 0
Number of ipv4 entry recreate success           : 1
Number of ipv4 entry recreate failed            : 0
Number of ipv6 entry recreate success           : 0
Number of ipv6 entry recreate failed            : 0
Number of partial delete received               : 0
```

```
Number of client purge attempted               : 0
Number of heap and db entry purge success      : 0
Number of purge success for db entry only      : 0
Number of client purge failed                  : 0
Number of garp sent                            : 1
Number of garp failed                          : 0
Number of IP entries validated in cleanup      : 0
Number of IP entry address errors in cleanup   : 0
Number of IP entry deleted in cleanup          : 0
Number of IP entry delete failed in cleanup    : 0
Number of IP table create callbacks on standby  : 0
Number of IP table modify callbacks on standby  : 0
Number of IP table delete callbacks on standby  : 0
Number of MAC table create callbacks on standby : 1
Number of MAC table modify callbacks on standby : 0
Number of MAC table delete callbacks on standby : 0
```

To view the HA redundancy summary, use the following command:

```
Device# show wireless stat redundancy summary
HA redundancy summary
---------------------

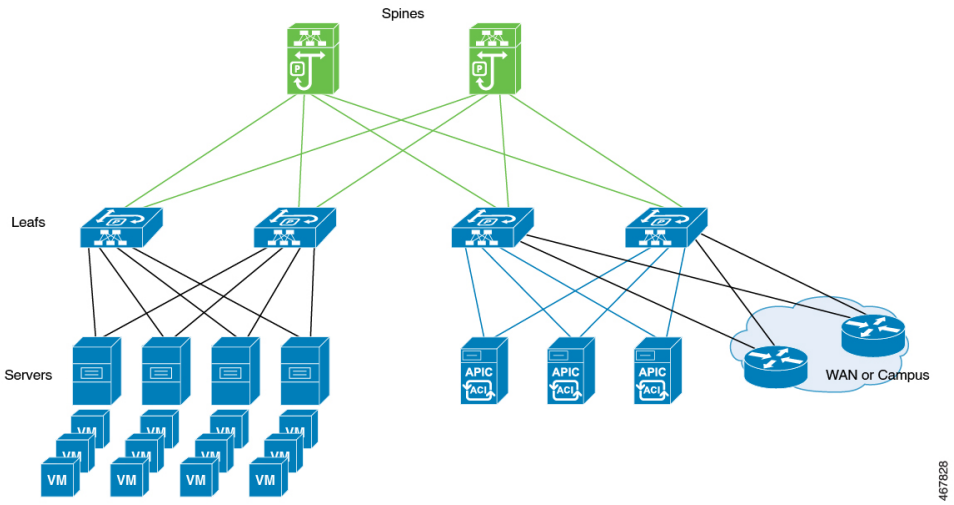
AP recovery duration (ms)        : 264
SSO HA sync timer expired        : No
```

Verifying High Availability

Table 102: Commands for Monitoring Chassis and Redundancy

Command Name	Description
show chassis	Displays the chassis information. **Note** When the peer timeout and retries are configured, the **show chassis ha-status** command output may show incorrect values. To check the peer keep-alive timer and retries, use the following commands: • **show platform software stack-mgr chassis active r0 peer-timeout** • **show platform software stack-mgr chassis standby r0 peer-timeout**
show redundancy	Displays details about Active box and Standby box.
show redundancy switchover history	Displays the switchover counts, switchover reason, and the switchover time.

To start the packet capture in the redundancy HA port (RP), use the following commands:

- test wireless redundancy packet dump start
- test wireless redundancy packet dump stop

- test wireless redundancy packet dump start filter port 2300

```
Device# test wireless redundancy packetdump start
Redundancy Port PacketDump Start
Packet capture started on RP port.

Device# test wireless redundancy packetdump stop
Redundancy Port PacketDump Start
Packet capture started on RP port.
Redundancy Port PacketDump Stop
Packet capture stopped on RP port.
Device# dir bootflash:
Directory of bootflash:/
1062881  drwx           151552  Oct 20 2020 23:15:25 +00:00  tracelogs
47       -rw-           20480  Oct 20 2020 23:15:24 +00:00  haIntCaptureLo.pcap
1177345  drwx             4096  Oct 20 2020 19:56:14 +00:00  certs
294337   drwx             8192  Oct 20 2020 19:56:05 +00:00  license_evlog
15       -rw-              676  Oct 20 2020 19:56:01 +00:00  vlan.dat
14       -rw-               30  Oct 20 2020 19:55:16 +00:00  throughput_monitor_params
13       -rw-           134808  Oct 20 2020 19:54:57 +00:00  memleak.tcl
1586145  drwx             4096  Oct 20 2020 19:54:45 +00:00  .inv
1103761  drwx             4096  Oct 20 2020 19:54:39 +00:00  dc_profile_dir
17       -r--              114  Oct 20 2020 19:54:17 +00:00  debug.conf
1389921  drwx             4096  Oct 20 2020 19:54:17 +00:00  .installer
46       -rw-       1104760207  Oct 20 2020 19:26:41 +00:00  leela_katar_rping_test.SSA.bin
49057    drwx             4096  Oct 20 2020 16:11:21 +00:00  .prst_sync
45       -rw-       1104803200  Oct 20 2020 15:39:19 +00:00
C9800-L-universalk9_wlc.2020-10-20_14.57_yavadhan.SSA.bin
269809   drwx             4096  Oct 19 2020 23:41:49 +00:00  core
44       -rw-       1104751981  Oct 19 2020 17:42:12 +00:00
C9800-L-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20201018_053825_2.SSA.bin
43       -rw-       1104286975  Oct 16 2020 12:05:47 +00:00
C9800-L-universalk9_wlc.BLD_POLARIS_DEV_LATEST_20201010_001654_2.SSA.bin

Device# test wireless redundancy packetdump start filter port 2300
Redundancy Port PacketDump Start
Packet capture started on RP port with port filter 2300.
```

To check connection between the two HA Ports (RP) and check if there are any drops, delays, or jitter in the connection, use the following command:

```
Device# test wireless redundancy rping
Redundancy Port ping
PING 169.254.64.60 (169.254.64.60) 56(84) bytes of data.
64 bytes from 169.254.64.60: icmp_seq=1 ttl=64 time=0.083 ms
64 bytes from 169.254.64.60: icmp_seq=2 ttl=64 time=0.091 ms
64 bytes from 169.254.64.60: icmp_seq=3 ttl=64 time=0.074 ms

--- 169.254.64.60 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2041ms
rtt min/avg/max/mdev = 0.074/0.082/0.091/0.007 ms
test wireless redundancy
```

To see the HA port interface setting status, use the **show platform hardware slot R0 ha_port interface stats** command.

```
Device# show platform hardware slot R0 ha_port interface stats
HA Port
ha_port   Link encap:Ethernet  HWaddr 70:18:a7:c8:80:70
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

```
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:e0900000-e0920000

Settings for ha_port:
        Supported ports:            [ TP ]
        Supported link modes:       10baseT/Half 10baseT/Full
                                    100baseT/Half 100baseT/Full
                                    1000baseT/Full
        Supported pause frame use:   Symmetric
        Supports auto-negotiation:   Yes
        Supported FEC modes:         Not reported
        Advertised link modes:       10baseT/Half 10baseT/Full
                                     100baseT/Half 100baseT/Full
                                     1000baseT/Full
        Advertised pause frame use:  Symmetric
        Advertised auto-negotiation: Yes
        Advertised FEC modes:        Not reported
        Speed:                       Unknown!
        Duplex:                      Unknown! (255)
        Port:                        Twisted Pair
        PHYAD:                       1
        Transceiver:                 internal
        Auto-negotiation:            on
        MDI-X:                       off (auto)
        Supports Wake-on:            pumbg
        Wake-on:                     g
        Current message level:       0x00000007 (7)
                                     drv probe link
        Link detected:               no

NIC statistics:
     rx_packets:             0
     tx_packets:             0
     rx_bytes:               0
     tx_bytes:               0
     rx_broadcast:           0
     tx_broadcast:           0
     rx_multicast:           0
     tx_multicast:           0
     multicast:              0
     collisions:             0
     rx_crc_errors:          0
     rx_no_buffer_count:     0
     rx_missed_errors:       0
     tx_aborted_errors:      0
     tx_carrier_errors:      0
     tx_window_errors:       0
     tx_abort_late_coll:     0
     tx_deferred_ok:         0
     tx_single_coll_ok:      0
     tx_multi_coll_ok:       0
     tx_timeout_count:       0
     rx_long_length_errors:  0
     rx_short_length_errors: 0
     rx_align_errors:        0
     tx_tcp_seg_good:        0
     tx_tcp_seg_failed:      0
     rx_flow_control_xon:    0
     rx_flow_control_xoff:   0
     tx_flow_control_xon:    0
     tx_flow_control_xoff:   0
     rx_long_byte_count:     0
     tx_dma_out_of_sync:     0
     tx_smbus:               0
```

```
rx_smbus:               0
dropped_smbus:          0
os2bmc_rx_by_bmc:       0
os2bmc_tx_by_bmc:       0
os2bmc_tx_by_host:      0
os2bmc_rx_by_host:      0
tx_hwtstamp_timeouts:   0
rx_hwtstamp_cleared:    0
rx_errors:              0
tx_errors:              0
tx_dropped:             0
rx_length_errors:       0
rx_over_errors:         0
rx_frame_errors:        0
rx_fifo_errors:         0
tx_fifo_errors:         0
tx_heartbeat_errors:    0
tx_queue_0_packets:     0
tx_queue_0_bytes:       0
tx_queue_0_restart:     0
tx_queue_1_packets:     0
tx_queue_1_bytes:       0
tx_queue_1_restart:     0
rx_queue_0_packets:     0
rx_queue_0_bytes:       0
rx_queue_0_drops:       0
rx_queue_0_csum_err:    0
rx_queue_0_alloc_failed:0
rx_queue_1_packets:     0
rx_queue_1_bytes:       0
rx_queue_1_drops:       0
rx_queue_1_csum_err:    0
rx_queue_1_alloc_failed:0
```

High Availability Deployment for Application Centric Infrastructure (ACI) Network

Information About Deploying ACI Network in Controller

Cisco Application Centric Infrastructure (ACI) technology integrates virtual and physical workloads in a programmable and multihypervisor fabric to build a multiservice or a cloud data center.

Note The Cisco ACI technology is supported only in a Redundancy Management Interface (RMI) high-availability network.

The following figure depicts the discrete components connected in a spine and leaf switch topology provisioned and managed as a single entity.

Figure 46: Cisco ACI Network Deployment



The following mechanisms help avoid interleaving traffic.

Bringing Down Wireless Management Interface Faster

In case of a switchover in ACI deployments, APs and clients are dropped because of interleaving traffic between the old and the new active controller. To resolve this issue, bring down the traffic from the old active controller faster. You can do this by bringing down the wireless management interface as soon as a failure is detected. When the wireless management interface shuts down, the traffic that is sourced from the old active wireless management interface stops. This avoids conflicts in the management IP address. The standby controller transitions to the role of the active controller with a new IP-MAC binding.

Note The IP Data-Plane Learning feature in an ACI deployment tracks the following:

- A duplicate MAC address for the same IP.
- Alarm that blocks the IP address for a configured duration.

During failure detection, the controller sets up the chassis property **non-participant**. In IP Data-Plane Learning feature, listen to the property for bringing down the wireless management interface and shutting down traffic in the old active controller faster, thereby avoiding any kind of interleaving traffic between the old and new active controllers.

Disabling Fast Switchover Notification

This mechanism provides more control to avoid interleaving traffic.

During failure handling, the active controller sends an explicit notification to the standby controller, stating that it is going down. This triggers the standby node to take over as the active node. In the event of failure, you can use the disable fast switchover notification option to control the explicit notification from active to standby. In the absence of explicit notification, the standby controller takes over as the active controller on the basis of keepalive timeout.

Note You can configure the keepalive timeout so that you have control over when the traffic from the new active controller begins if a failure occurs. In such a failure scenario, the switchover also gets delayed.

When you enable this option, the active controller cannot send an explicit failure notification message to the standby controller. The standby controller relies solely on the keepalive timeout failures to detect when the active controller went down.

This delays the keepalive timeout in the commencing traffic in the new active controller, thus avoiding the overlapping traffic from the old active controller. Therefore, disabling fast switchover notification increases the switchover duration by the additional keepalive timeout duration.

GARP Burst

During a controller switchover event, the GARP traffic is generated in burst that overwhelms the ARP learning of ACI. This feature devises a way to retransmit the GARP packet at a much lower rate after a switchover from a new active controller.

Prerequisite for Deploying the ACI Network in the Controller

Check the maximum supported clients in High Availability to ensure that Cisco ACI does not exceed the configured IPv4 and IPv6 end points.

Disabling the Fast Switchover Notification Mechanism (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no redun-management fast-switchover** **Example:** `Device(config)# no redun-management fast-switchover`	Disables explicit fast switchover notification. **Note** Configure the fast switchover notification mechanism in the primary controller. This configuration is not required in the secondary controller.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring Gratuitous ARP (GARP) Retransmit (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**redun-management garp-retransmit burst** *packet-burst-size* **interval** *time-interval* **Example:** `Device(config)# redun-management garp-retransmit burst 0 interval 0`	Determines the rate at which the GARP resend is performed. **Note** • *packet-burst-size*: The valid range is from 0 to 1000. The value 0 refers to the disabled retransmit. • *time-interval*: Refers to the time interval, in seconds. The valid range is from 0 to 5 seconds. The value 0 refers to the disabled retransmit.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Disabling Initial GARP (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no redun-management garp-retransmit initial** **Example:** `Device(config)# no redun-management garp-retransmit initial`	Disables the initial GARP.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring a Switchover

Procedure

	Command or Action	Purpose
Step 1	**To force a failover to the standby unit, use the following command:** **Example:** `Device#redundancy force-switchover`	In this case, the standby controller will take the role of the active controller, and the active controller will reload and become the new standby controller. This command can be used to test the stability of the high availability cluster and see if switchovers are working as expected. **Note** Do not use any other command to test switchovers between the Cisco Catalyst 9800 series wireless controllers. Command such as "reload slot X" (where X is the active controller) might lead to unexpected behaviour and should not be used to perform a switchover.

Information About Redundancy Management Interface

The Redundancy Management Interface (RMI) is used as a secondary link between the active and standby Cisco Catalyst 9800 Series Wireless Controllers. This interface is the same as the wireless management interface, and the IP address on this interface is configured in the same subnet as the Wireless Management IP. The RMI is used for the following purposes:

- Dual Active Detection
- Exchange resource health information between controllers, for instance, gateway reachability status from either controller.
- Gateway reachability is checked on the active and the standby controller through the RMI when the feature is enabled. It takes approximately the configured gateway monitoring interval to detect that a controller has lost gateway reachability. The default gateway monitoring interval value is 8 seconds.

Note

- The RMI might trigger a switchover based on the gateway status of the active controller.
- Cisco TrustSec is not supported on the RMI.

  When the device SGT is used, the IP-SGT mapping for RMI address is also applied along with the WMI address. So, you need to ensure that the SGACL is defined appropriately to allow ICMP and ARP traffic between the active and standby RMI addresses.
- If the RP and RMI links are down, the HA setup breaks into two active controllers. This leads to IP conflict in the network. The HA setup forms again when the RP link comes up. Depending on the state of the external switch at this time, the ARP table may or may not be updated to point to the active controller. That is, the switch may fail to process the GARP packets from the controller. As a best practice, we recommend that you keep the ARP cache timeout value to a low value for faster recovery from multiple fault scenarios. You need to select a value that does not impact the network traffic, for instance, 30 minutes.

Note The AAA packets originating from the controller may use either the wireless management IP or the RMI IP. Therefore, ensure that you add RMI IP as the source IP along with WMI IP in the AAA server.

Active Controller

The primary address on the active controller is the management IP address. The secondary IPv4 address on the management VLAN is the RMI IP address for the active controller. Do not configure the secondary IPv4 addresses explicitly because a single secondary IPv4 address is configured automatically by RMI under the RMI.

Standby Controller

The standby controller does not have the wireless management IP configured; it has the RMI IP address configured as the primary IP address. When the standby controller becomes active, the management IP address becomes the primary IP address and the RMI IP address becomes the secondary IP address. If the interface on the active controller is administratively down, the same state is reflected on the standby controller.

Dual Stack Support on Management VLAN with RMI

Dual stack refers to the fact that the wireless management interface can be configured with IPv4 and IPv6 addresses. If an RMI IPv4 address is configured along with an IPv4 management IP address, you can additionally configure an IPv6 management address on the wireless management interface. This IPv6 management IP address will not be visible on the standby controller.

If an RMI IPv6 address is configured along with an IPv6 management IP address, you can additionally configure an IPv4 management address on the wireless management interface. This IPv4 management IP address will not be visible on the standby controller.

Therefore, you can monitor only the IPv6 gateway when the RMI IPv6 address is configured, or only the IPv4 gateway when the RMI IPv4 address is configured.

Note The RMI feature supports the RMI IPv4 or IPv6 addresses.

RMI-Based High-Availability Pairing

You should consider the following scenarios for HA pairing:

- Fresh Installation
- Already Paired Controllers
- Upgrade Scenario
- Downgrade Scenario

Dynamic HA pairing requires both the active controller and the standby controller to reload. However, dynamic HA pairing occurs on the Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, and the Cisco Catalyst 9800-80 Wireless Controller when one of them reloads and becomes the standby controller.

Note Chassis numbers identify individual controllers. Unique chassis numbers must be configured before forming an HA pair.

HA Pairing Without Previous Configuration

When HA pairing is done for the first time, no ROMMON variables are found for the RP IP addresses. You can choose from the existing privileged EXEC mode RP-based commands or the RMI IP-based mechanisms. However, the privileged EXEC mode RP-based commands will be deprecated soon. If you use Cisco Catalyst Center, you can choose the privileged EXEC mode RP-based CLI mechanism till the Cisco Catalyst Center migrates to support the RMI.

The RP IPs are derived from the RMI IPs after an HA pair is formed. Also, the privileged EXEC mode RP-based CLI method of clearing and forming an HA pair is not allowed after the RMI IP-based HA mechanism is chosen.

Note

- Although you can choose RP or RMI for a fresh installation, we recommend that you use RMI install method.
- To view the ROMMON variables, use the **show romvars** command.

If you choose the privileged EXEC RP-based CLI mechanism, the RP IPs are configured the same way as in the 16.12 release.

The following occurs when the RMI-based HA pairing is done on a brand-new system:

- RP IPs are derived from RMI IPs and used in HA pairing.
- Privileged EXEC mode RP-based CLIs are blocked.

Note The RMI migration is supported from Cisco Catalyst Center, 2.3.3.x release version.

The following are the limitations observed during RMI migration:

- The negative cases fail due to the following reasons:
  - When devices are not reachable.
  - When non-Cisco Catalyst 9800 Series Wireless Controllers are in use.
  - When an earlier controller version (Cisco IOS XE 17.3) is in use.
  - When High Availability is not configured.
  - When High Availability RMI is already configured.
- When High Availability is upgraded to RMI-based High Availability for Cisco IOS XE release version greater than or equal to 17.3.
- When upgrading to an already failed High Availability paired controller.
- The controller GUI prohibits applying RMI migration configuration to High Availability failed devices.

Paired Controllers

If the controllers are already in an HA pair, the existing EXEC mode RP-based commands will continue to be used. You can enable RMI to migrate to the RMI-based HA pairing.

If the controllers are already paired and RMI is configured, it will overwrite the RP IPs with the RMI-derived IPs. The HA pair will not be disturbed immediately, but the controllers will pick up the new IP when the next reload happens. The RMI feature mandates a reload for the feature to be effective. When both the controllers are reloaded, they come up as a pair with the new RMI-derived RP IPs.

The following occurs when the RMI configuration is done:

- The RP IPs derived from the RMI IPs are overwritten, and used for HA pairing.
- If the active and standby controller already exist prior to HA pairing through the EXEC mode RP-based command mechanism, the pair is not interrupted.
- When the pair reloads later, the new RP IPs are used.
- EXEC mode RP-based commands are blocked.

Upgrading from Cisco IOS XE 16.1.x to a Later Release

A system that is being upgraded can choose to:

- Migrate with the existing RP IP configuration intact—In this case, the existing RP IP configuration will continue to be used. The EXEC mode RP-based commands are used for future modifications.
- Migrate after clearing the HA configuration—In this case, you can choose between the old (EXEC mode RP-based commands) and new RMI-based RP configuration methods.

Note In case the older configuration is retained, the RMI configuration updates the RP IPs with the IPs derived from the RMI IPs.

Downgrade Scenario

Note The downgrade scenario given below is not applicable for Cisco IOS XE Amsterdam 17.1.x.

The downgrade scenario will have only the EXEC mode RP-based commands. The following are the two possibilities:

- If the upgraded system used the RMI-based RP configuration.
- If the upgraded system continued to use the EXEC mode RP-based commands.

Note In the above cases, the downgraded system uses the EXEC mode RP-based commands to modify the configuration. However, the downgraded system will continue to use the new derived RP IPs.

Note When you downgrade the Cisco Catalyst 9800 Series Wireless Controller to any version below 17.1 and if the mDNS gateway is enabled on the WLAN/RLAN/GLAN interfaces, the mdns-sd-interface gateway goes down after the downgrade.

To enable the mDNS gateway on the WLAN/RLAN/GLAN interfaces in 16.12 and earlier versions, use the following commands:

wlan test 1 test

mdns-sd gateway

To enable the mDNS gateway on the WLAN/RLAN/GLAN interfaces from version 17.1 onwards, use the following command:

mdns-sd-interface gateway

Gateway Monitoring

From Cisco IOS XE Amsterdam 17.2.1 onwards, the method to configure the gateway IP has been modified. The **ip default-gateway** *gateway-ip* command is not used. Instead, the gateway IP is selected based on the static routes configured. From among the static routes configured, the gateway IP that falls in the same subnet as the RMI subnet (the broadest mask and least gateway IP) is chosen. If no matching static route is found, gateway failover will not work (even if management gateway-failover is enabled).

Configuring Redundancy Management Interface (GUI)

Before you begin

Before configuring RMI + RP using GUI, ensure that WMI is available.

Procedure

Step 1 In the **Administration > Device > Redundancy** window, perform the following:

a. Set the **Redundancy Configuration** toggle button to **Enabled** to activate redundancy configuration.

b. In the **Redundancy Pairing Type** field, select **RMI+RP** to perform RMI+RP redundancy pairing as follows:

- In the **RMI IP for Chassis 1** field, enter RMI IP address for chassis 1.
- In the **RMI IP for Chassis 2** field, enter RMI IP address for chassis 2.
- From the **HA Interface** drop-down list, choose one of the HA interface.

  Note You can select the HA interface only for Cisco Catalyst 9800 Series Wireless Controllers.

- Set the **Management Gateway Failover** toggle button to **Enabled** to activate management gateway failover.
- In the **Gateway Failure Interval** field, enter an appropriate value. The valid range is between 6 and 12 (seconds). The default is 8 seconds.

c. In the **Redundancy Pairing Type** field, select **RP** to perform RP redundancy pairing as follows:

- In the **Local IP** field, enter an IP address for Local IP.
- In the **Netmask** field, enter the subnet mask assigned to all wireless clients.
- From the **HA Interface** drop-down list, choose one of the HA interface.

  Note You can select the HA interface only for Cisco Catalyst 9800 Series Wireless Controllers.

- In the **Remote IP** field, enter an IP address for Remote IP.

d. In the **Keep Alive Timer** field, enter an appropriate timer value. The valid range is between 1 and 10 (x100 milliseconds).

e. In the **Keep Alive Retries** field, enter an appropriate retry value. The valid range is between 3 and 10 seconds.

f. In the **Active Chassis Priority** field, enter a value.

Step 2 Click **Apply** and reload controllers.

Configuring Redundancy Management Interface (CLI)

Procedure

	Command or Action	Purpose
Step 1	**chassis** *chassis-num* **priority** *chassis-priority* **Example:** `Device# chassis 1 priority 1`	(Optional) Configures the priority of the specified device. **Note** From Cisco IOS XE Gibraltar 16.12.x onwards, device reload is not required for the chassis priority to become effective. • *chassis-num*—Enter the chassis number. The range is from 1 to 2. • *chassis-priority*—Enter the chassis priority. The range is from 1 to 2. The default value is 1. **Note** When both the devices boot up at the same time, the device with higher priority becomes active, and the other one becomes standby. If both the devices are configured with the same priority value, the one with the smaller MAC address acts as active and its peer acts as standby.
Step 2	**chassis redundancy ha-interface GigabitEthernet** *interface-number* **Example:** `Device# chassis redundancy ha-interface GigabitEthernet 3`	Creates an HA interface for your controller. • *interface-number*: GigabitEthernet interface number. The range is from 1 to 32. **Note** This step is applicable only for Cisco Catalyst 9800-CL Series Wireless Controllers. The chosen interface is used as the dedicated interface for HA communication between the 2 controllers.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**redun-management interface vlan** *vlan-interface-number* **chassis** *chassis-number*	Configures Redundancy Management Interface.

	Command or Action	Purpose
	address *ip-address* **chassis** *chassis-number* **address** *ip-address* **Example:** `Device(config)# redun-management interface Vlan 200 chassis 1 address 9.10.90.147 chassis 2 address 9.10.90.149`	• *vlan-interface-number* : VLAN interface number. The valid range is from 1 to 4094. **Note** Here, the *vlan-interface-number* is the same VLAN as the Management VLAN. That is, both must be on the same subnet. • *chassis-number*: Chassis number. The valid range is from 1 to 2. • *ip-address*: Redundancy Management Interface IP address. **Note** Each controller must have a unique chassis number for RMI to form the HA pair. The chassis number can be observed as SWITCH_NUMBER in the output of **show romvar** command. Modification of SWITCH_NUMBER is currently not available through the web UI. To disable the HA pair, use the **no redun-management interface vlan chassis** command.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**write memory** **Example:** `Device# write memory`	Saves the configuration.
Step 7	**reload** **Example:**	Reloads the controllers.

	Command or Action	Purpose
	`Device# reload`	**Note** When the RMI configuration is done, you must reload the controllers for the configuration to take effect. For Cisco Catalyst 9800-CL Wireless Controller VM, both the active and standby controllers reload automatically. In the case of hardware platforms, you should reload the active controller manually, as only standby the controller reloads automatically.

Configuring Gateway Monitoring (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **management gateway-failover enable** **Example:** `Device(config)# management gateway-failover enable`	Enables gateway monitoring. (Use the **no** form of this command to disable gateway monitoring.)
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. **Note** To save the configuration, use the **write memory** command.

Configuring Gateway Monitoring Interval (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**management gateway-failover interval** *interval-value* **Example:** `Device(config)# management gateway-failover interval 6`	Configures the gateway monitoring interval. *interval-value* - Refers to the gateway monitoring interval. The valid range is from 6 to 12. Default value is 8.
Step 3	**end** **Example:** `Device(config)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

Gateway Reachability Detection

Information About Gateway Reachability Detection

Gateway Reachability Detection feature mimimizes the downtime on APs and clients when the gateway reachability is lost on the active controller.

Both active and standby controllers keep track of gateway reachability. The gateway reachability is detected by sending Internet Control Message Protocol (ICMP) and ARP requests periodically to the gateway.

Both active and standby controllers use the RMI IP as the source IP. The messages are sent at 1 second interval. If it takes 8 (or configured value) consecutive failures in reaching the gateway, the controller declares the gateway as non-reachable. It takes approximately 8 seconds to detect if a controller has lost gateway reachability.

Gateway monitoring with native IPv6 uses ICMP Neighbor Discovery protocols and ICMPv6 ECHO to check gateway reachability.

Therefore, you can monitor only the IPv6 gateway when RMI IPv6 is configured.

This means that only one IPv4 or IPv6 gateways can be monitored.

Note If the standby controller loses gateway, the standby moves to the standby recovery mode.

If the active controller loses gateway, the active reloads and standby becomes active.

Configuration Workflow

1. Configuring Redundancy Management Interface (GUI) (or) Configuring Redundancy Management Interface (CLI). For more information, see Configuring Redundancy Management Interface (GUI), on page 1484.

Note For RMI configuration to take effect, ensure that you reload your controllers.

2. Configuring IPv6 Static Route. For information, see Gateway Monitoring.

3. Configuring Gateway Monitoring Interval (CLI). For more information, see Configuring Gateway Monitoring Interval (CLI), on page 1487.

Migrating to RMI IPv6

From RMI IPv4

1. Unconfigure the RMI IPv4 using the following CLIs:

```
Device# conf t
Device(config)# no redun-management interface <vlan_name> chassis 1 address <ip_address1>
 chassis 2 address <ip_address2>
```

Note This CLI unconfigures RMI on both the controllers.

2

Note Take a backup of the running config on active before you reload the controller.

Reload the controller.

3. Copy the backed up config to the running config on the box which would have lost all the config.
4. Configure the RMI IPv6 on both the controllers. For information on the CLI, see #unique_1845.
5. Reload the controller.

From HA Pairing (Without RMI)

For information on HA pairing, see Configuring Redundancy Management Interface (GUI).

Monitoring the Health of the Standby Controller

The Standby Monitoring feature allows you to monitor the health of a system on a standby controller using programmatic interfaces and commands. This feature allows you to monitor parameters such as CPU, memory, interface status, power supply, fan failure, and the system temperature. Standby Monitoring is enabled when Redundancy Management Interface (RMI) is configured, no other configuration is required. The RMI itself is used to connect to the standby and perform standby monitoring. Standby Monitoring feature cannot be dynamically enabled or disabled.

Note The active controller uses the management or RMI IP to initiate AAA requests. Whereas, the standby controller uses the RMI IP to initiate AAA requests. Thus, the RMI IPs must be added in AAA servers for a seamless client authentication and standby monitoring.

To enable standby console, ensure that the following configuration is in place:

```
redundancy
main-cpu
secondary console enable
```

Note The Standby Monitoring feature is not supported on a controller in the active-recovery and the standby-recovery modes.

The Standby Monitoring feature supports only the following traffic on the RMI interface of the standby controller:

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- TCP Traffic (to or from) ports: 22, 443, 830, and 3200
- UDP RADIUS ports:1645 and1646
- UDP Extended RADIUS ports: 21645 to 21844

Feature Scenarios

- To monitor the health of the standby directly from the standby controller using Standby RMI IP.
- To get syslogs from the standby controller using the Standby RMI IP.

Use Cases

- Enabling SNMP agent and programmatic interfaces on the standby controller: You can directly perform an SNMP query or programmatic interface query to the standby's RMI IP and active controller.
- Enabling syslogs on the standby controller: You can directly get the standby syslogs from the standby controller.

RADIUS Accounting Support

Whenever you log in to a standby device, the RADIUS start record must be sent to the external RADIUS server. Similarly, when you log out of a device, the RADIUS stop record must be sent to the external RADIUS server.

TACACS+ Authentication Support

Users are authenticated through the RMI using the external TACACS+ server. The username and password are evaluated in the TACACS+ server. Depending on the response received from the server, a user will be able to log in to the standby device.

TACACS+ Accounting Support

Whenever you log in to the standby device, the TACACS+ accounting start record must be sent to the external TACACS+ server. Similarly, when you log out of a device, the TACACS+ accounting stop record must be sent to the external TACACS+ server.

Note The following configuration must be in place to configure AAA to send the accounting packets:

```
aaa accounting exec {default | named-list} start-stop group {RAD | tac-group-name}
```

Note The TACACS+ login to the standby device is not supported when TACACS+ server is configured with hostname.

Monitoring the Health of Standby Parameters Using SNMP

Standby Monitoring Using Standby RMI IP

When an SNMP agent is enabled on the standby controller, you can directly perform an SNMP query to the standby's RMI IP. From Release 17.5 onwards, you can query the following MIB on the standby controller:

Table 103: MIB Name and Notes

MIB Name	Notes
IF-MIB	This MIB is used to monitor the interface statistics of the standby controller using the standby RMI IP address.

Note If an SNMP agent is enabled on the active controller, by default, the SNMP is enabled on the standby controller.

Standby Monitoring Using the Active Controller

CISCO-LWAPP-HA-MIB

The CISCO-LWAPP-HA-MIB monitors the health parameters of the standby controller, that is, memory, CPU, port status, power statistics, peer gateway latencies, and so on.

You can query the following MIB objects of CISCO-LWAPP-HA-MIB.

Table 104: MIB Objects and Notes

MIB Objects	Notes
cLHaPeerHotStandbyEvent	This object can be used to check if the standby controller has turned hot-standby or not.
cLHaBulkSyncCompleteEvent	This object represents the time at which the bulksync is completed.

CISCO-PROCESS-MIB

The CISCO-PROCESS-MIB monitors CPU and process statistics. Use it to monitor CPU-related or memory-related BINOS processes. The standby CISCO-PROCESS-MIB can be monitored using the active controller.

ENTITY-MIB

The ENTITY-MIB is used to monitor hardware details of the active and standby controllers using the active controller.

Note The standby Route Processor (RP) sensors are appended in the active RP sensors.

Standby IOS Linux Syslogs

The standby logs are relayed using the same method as on the active Cisco IOS for wireless controllers.

From Release 17.5 onwards, external logging of syslogs from the standby IOS is enabled. As BINOS processes on standby also forwards the syslogs to Cisco IOS, all the syslogs generated on the standby controller is forwarded to the configured external server.

Note RMI IP address is used for logging purpose.

The following is the expected behavior when an HA pair is configured with the RMI IPv6 address, the active controller has dual stack, and logging is configured on the IPv4 address:

The standby controller tries to send syslogs to the IPv4 server because logging is only configured on IPv4 even though IPv4 is not supported by standby.

Standby Interface Status Using Active SNMP

The standby interface information is sent to the active controller using IPC in the following scenarios:

- When there is a change in the interface status.
- When a new interface is added or deleted on the standby controller.

When the active controller receives the interface information from the standby controller, the active controller's database is populated with the standby interface information.

When an SNMP query is received for the standby interface information, the SNMP handlers corresponding to the CISCO-LWAPP-HA-MIB reads them from the standby interface database on the active and populates the MIB objects in CISCO-LWAPP-HA-MIB.

You can query the following MIB objects of CISCO-LWAPP-HA-MIB.

Table 105: MIB Objects of CISCO-LWAPP-HA-MIB

MIB Object	Notes
stbyIfIndex	This is a unique value (greater than zero) for each interface of the standby controller.
stbyIfName	This is the name of the standby interface.
stbyIfPhysAddress	This is the interface address of the standby controller in the protocol sublayer.
stbyifOperStatus	This is the current operational state of the interface in the standby controller.
stbyifAdminStatus	This is the desired state of the interface of the standby controller.

To verify the logging on the active when the standby fails to send interface statistics, use the following command:

```
Device# debug snmp ha-chkpt
Device# debug snmp ha-intf_db
```

Monitoring the Health of Standby Controller Using Programmatic Interfaces

You can monitor parameters such as CPU, memory, sensors, and interface status on a standby controller using programmatic interfaces such as NETCONF and RESTCONF. The RMI IP of the standby controller can be used for access to the following operational models:

The models can be accessed through .

- Cisco-IOS-XE-device-hardware-oper.yang
- Cisco-IOS-XE-process-cpu-oper.yang
- Cisco-IOS-XE-platform-software-oper.yang
- Cisco-IOS-XE-process-memory-oper.yang
- Cisco-IOS-XE-interfaces-oper.yang

For more information on the YANG models, see the *Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.3.x*.

Monitoring the Health of Standby Controller Using CLI

This section describes the different commands that can be used to monitor the standby device.

You can connect to the standby controller through SSH using the RMI IP of the standby controller. The user credentials must have been configured already. Both local authentication and RADIUS authentication are supported.

Note The **redun-management** command needs to be configured on both the controllers, primary and standby, prior to high availability (HA) pairing.

Monitoring Port State

The following is a sample output of the **show interfaces** *interface-name* command:

```
Device-standby# show interfaces GigabitEthernet1

GigabitEthernet1 is down, line protocol is down
Shadow state is up, true line protocol is up
  Hardware is CSR vNIC, address is 000c.2909.33c2 (bia 000c.2909.33c2)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is force-up, media type is Virtual
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:06, output 00:00:24, output hang never
  Last clearing of "show interface" counters never
  Input queue: 30/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 389000 bits/sec, 410 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     3696382 packets input, 392617128 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     18832 packets output, 1218862 bytes, 0 underruns
     Output 0 broadcasts (0 multicasts)
     0 output errors, 0 collisions, 2 interface resets
     3 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The following is a sample output of the **show ip interface brief** command:

```
Device# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES unset  down                  down
GigabitEthernet0       unassigned      YES NVRAM  administratively down down
Capwap1                unassigned      YES unset  up                    up
Capwap2                unassigned      YES unset  up                    up
Capwap3                unassigned      YES unset  up                    up
Capwap10               unassigned      YES unset  up                    up
Vlan1                  unassigned      YES NVRAM  down                  down
Vlan56                 unassigned      YES unset  down                  down
Vlan111                111.1.1.85      YES NVRAM  up                    up
```

Monitoring CPU or Memory

The following is a sample output of the **show process cpu sorted 5sec** command:

```
Device-standby# show process cpu sorted 5sec

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  10     1576556      281188       5606  0.15%  0.05%  0.05%   0 Check heaps
 232      845057    54261160         15  0.07%  0.05%  0.06%   0 IPAM Manager
 595         177         300        590  0.07%  0.02%  0.01%   2 Virtual Exec
 138     1685973   108085955         15  0.07%  0.08%  0.08%   0 L2 LISP Punt Pro
 193       19644      348767         56  0.07%  0.00%  0.00%   0 DTP Protocol
   5           0           1          0  0.00%  0.00%  0.00%   0 CTS SGACL db cor
   4          24          15       1600  0.00%  0.00%  0.00%   0 RF Slave Main Th
   6           0           1          0  0.00%  0.00%  0.00%   0 Retransmission o
   7           0           1          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   2      117631      348801        337  0.00%  0.00%  0.00%   0 Load Meter
   8           0           1          0  0.00%  0.00%  0.00%   0 EDDRI_MAIN
```

To check CPU and memory utilization of binOS processes, run the following command:

```
Device-standby# show platform software process slot chassis standby R0 monitor

top - 23:24:14 up 8 days, 3:38, 0 users, load average: 0.69, 0.79, 0.81
Tasks: 433 total, 1 running, 431 sleeping, 1 stopped, 0 zombie
%Cpu(s): 1.7 us, 2.8 sy, 0.0 ni, 95.6 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 32059.2 total, 21953.7 free, 4896.8 used, 5208.6 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 26304.6 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
23565 root 20 0 2347004 229116 130052 S 41.2 0.7 5681:44 ucode_pkt+
2306 root 20 0 666908 106760 46228 S 5.9 0.3 15:06.14 smand
22807 root 20 0 3473004 230020 152120 S 5.9 0.7 510:56.90 fman_fp_i+
1 root 20 0 14600 11324 7424 S 0.0 0.0 0:31.07 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.28 kthreadd
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/0+
7 root 20 0 0 0 0 I 0.0 0.0 0:00.49 kworker/u+
8 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu+
9 root 20 0 0 0 0 S 0.0 0.0 0:03.26 ksoftirqd+
.
.
.
32258 root 20 0 57116 3432 2848 S 0.0 0.0 0:00.00 rotee
32318 root 20 0 139560 9500 7748 S 0.0 0.0 0:55.67 pttcd
32348 root 20 0 31.6g 3.1g 607364 S 0.0 9.8 499:12.04 linux_ios+
32503 root 20 0 3996 3136 2852 S 0.0 0.0 0:00.00 stack_snt+
32507 root 20 0 3700 1936 1820 S 0.0 0.0 0:00.00 sntp
```

Monitoring Hardware

The following is a sample output of the **show environment summary** command:

```
Device# show environment summary


Number of Critical alarms:  0
Number of Major alarms:     0
Number of Minor alarms:     0

 Slot        Sensor          Current State   Reading
```

```
Threshold(Minor,Major,Critical,Shutdown)
 ----------  --------------  --------------- ------------
---------------------------------------
 P0          Vin             Normal          231  V AC    na
 P0          Iin             Normal          2    A       na
 P0          Vout            Normal          12   V DC    na
 P0          Iout            Normal          30   A       na
 P0          Temp1           Normal          25   Celsius (na ,na ,na ,na )(Celsius)
 P0          Temp2           Normal          31   Celsius (na ,na ,na ,na )(Celsius)
 P0          Temp3           Normal          37   Celsius (na ,na ,na ,na )(Celsius)
 R0          VDMB1: VX1      Normal          1226 mV      na
 R0          VDMB1: VX2      Normal          6944 mV      na
 R0          Temp: DMB IN    Normal          26   Celsius (45 ,55 ,65 ,70 )(Celsius)
 R0          Temp: DMB OUT   Normal          40   Celsius (70 ,75 ,80 ,85 )(Celsius)
 R0          Temp: Yoda 0    Normal          54   Celsius (95 ,105,110,115)(Celsius)
 R0          Temp: Yoda 1    Normal          62   Celsius (95 ,105,110,115)(Celsius)
 R0          Temp: CPU Die   Normal          43   Celsius (100,110,120,125)(Celsius)
 R0          Temp: FC FANS   Fan Speed 70%   26   Celsius (29 ,39 ,0  )(Celsius)
 R0          VDDC1: VX1      Normal          1005 mV      na
 R0          VDDC1: VX2      Normal          7084 mV      na
 R0          VDDC2: VH       Normal          12003mV      na
 R0          Temp: DDC IN    Normal          25   Celsius (55 ,65 ,75 ,80 )(Celsius)
 R0          Temp: DDC OUT   Normal          35   Celsius (75 ,85 ,95 ,100)(Celsius)
 P0          Stby Vin        Normal          230  V AC    na
 P0          Stby Iin        Normal          2    A       na
 P0          Stby Vout       Normal          12   V DC    na
 P0          Stby Iout       Normal          32   A       na
 P0          Stby Temp1      Normal          24   Celsius (na ,na ,na ,na )(Celsius)
 P0          Stby Temp2      Normal          29   Celsius (na ,na ,na ,na )(Celsius)
 P0          Stby Temp3      Normal          35   Celsius (na ,na ,na ,na )(Celsius)
 R0          Stby VDMB1: VX1 Normal          1225 mV      na
 R0          Stby VDMB1: VX2 Normal          6979 mV      na
 R0          Stby VDMB2: VX2 Normal          5005 mV      na
 R0          Stby VDMB2: VX3 Normal          854  mV      na
 R0          Stby VDMB3: VX1 Normal          972  mV      na
 R0          Stby Temp: DMB INormal          22   Celsius (45 ,55 ,65 ,70 )(Celsius)
 R0          Stby Temp: DMB ONormal          32   Celsius (70 ,75 ,80 ,85 )(Celsius)
 R0          Stby Temp: Yoda Normal          43   Celsius (95 ,105,110,115)(Celsius)
 R0          Stby Temp: Yoda Normal          45   Celsius (95 ,105,110,115)(Celsius)
 R0          Stby Temp: CPU DNormal          33   Celsius (100,110,120,125)(Celsius)
 R0          Stby Temp: FC FAFan Speed 70%   22   Celsius (29 ,39 ,0  )(Celsius)
 R0          Stby VDDC1: VX1 Normal          1005 mV      na
 R0          Stby VDDC1: VX2 Normal          7070 mV      na
 R0          Stby VDDC2: VX2 Normal          752  mV      na
 R0          Stby VDDC2: VX3 Normal          750  mV      na
 R0          Stby Temp: DDC INormal          22   Celsius (55 ,65 ,75 ,80 )(Celsius)
 R0          Stby Temp: DDC ONormal          28   Celsius (75 ,85 ,95 ,100)(Celsius)
```

Note The command displays both active and standby hardware details.

Note The **show environment summary** command displays data only for physical appliances such as Cisco Catalyst 9800-80 Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-L Wireless Controller, and Cisco Catalyst 9800 Embedded Wireless Controller for Switch. The command does not display data for Cisco Catalyst 9800 Wireless Controller for Cloud.

Verifying the Gateway-Monitoring Configuration

To verify the status of the gateway-monitoring configuration on an active controller, run the following command:

```
Device# show redundancy states

my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
Mode = Duplex
Unit = Primary
Unit ID = 1

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State = sso
Maintenance Mode = Disabled
Manual Swact = enabled
Communications = Up

client count = 129
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
Gateway Monitoring = Disabled
Gateway monitoring interval = 8 secs
```

To verify the status of the gateway-monitoring configuration on a standby controller, run the following command:

```
Device-stby# show redundancy states

my state = 8 -STANDBY HOT
peer state = 13 -ACTIVE
Mode = Duplex
Unit = Primary
Unit ID = 2

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State = sso
Maintenance Mode = Disabled
Manual Swact = cannot be initiated from this the standby unit
Communications = Up

client count = 129
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
Gateway Monitoring = Disabled
Gateway monitoring interval = 8 secs
```

Verifying the RMI IPv4 Configuration

Verify the RMI IPv4 configuration.

```
Device# show running-config interface vlan management-vlan

Building configuration...

Current configuration : 109 bytes
```

```
!
interface Vlan90
ip address 9.10.90.147 255.255.255.0 secondary
ip address 9.10.90.41 255.255.255.0
end
```

To verify the interface configuration for a standby controller, use the following command:

```
Device-stby# show running-config interface vlan 90

Building configuration...

Current configuration : 62 bytes
!
interface Vlan90
ip address 9.10.90.149 255.255.255.0
end
```

To verify the chassis redundancy management interface configuration for an active controller, use the following command:

```
Device# show chassis rmi

Chassis/Stack Mac Address : 000c.2964.1eb6 - Local Mac Address
Mac persistency wait time: Indefinite
   H/W Current
Chassis# Role      Mac Address     Priority  Version  State  IP             RMI-IP
-------------------------------------------------------------------------------------------
*1       Active    000c.2964.1eb6  1         V02      Ready  169.254.90.147 9.10.90.147
2        Standby   000c.2975.3aa6  1         V02      Ready  169.254.90.149 9.10.90.149
```

To verify the chassis redundancy management interface configuration for a standby controller, use the following command:

```
Device-stby# show chassis rmi

Chassis/Stack Mac Address : 000c.2964.1eb6 - Local Mac Address
Mac persistency wait time: Indefinite
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State  IP             RMI-IP
-------------------------------------------------------------------------------------------
1         Active   000c.2964.1eb6     1      V02     Ready  169.254.90.147  9.10.90.147
*2        Standby  000c.2975.3aa6     1      V02     Ready  169.254.90.149  9.10.90.149
```

To verify the ROMMON variables on an active controller, use the following command:

```
Device# show romvar | include RMI

RMI_INTERFACE_NAME = Vlan90
RMI_CHASSIS_LOCAL_IP = 9.10.90.147
RMI_CHASSIS_REMOTE_IP = 9.10.90.149
```

To verify the ROMMON variables on a standby controller, use the following command:

```
Device-stby# show romvar | include RMI

RMI_INTERFACE_NAME = Vlan90
RMI_CHASSIS_LOCAL_IP = 9.10.90.149
RMI_CHASSIS_REMOTE_IP = 9.10.90.147
```

To verify the switchover reason, use the following command:

```
Device# show redundancy switchover history

Index  Previous  Current  Switchover            Switchover
       active    active   reason                time
-----  --------  -------  ----------            ----------
   1       2        1     Active lost GW        17:02:29 UTC Mon Feb 3 2020
```

Verifying the RMI IPv6 Configuration

To verify the chassis redundancy management interface configuration for both active and standby controllers, run the following command:

```
Device# show chassis rmi

Chassis/Stack Mac Address : 00a3.8e23.a540 - Local Mac Address
Mac persistency wait time: Indefinite
Local Redundancy Port Type: Twisted Pair
                                                H/W   Current
Chassis#   Role     Mac Address    Priority Version State     IP             RMI-IP
-------------------------------------------------------------------------------------------

  1        Standby  706d.1536.23c0    1      V02     Ready  169.254.254.17   2020:0:0:1::211

 *2        Active   00a3.8e23.a540    1      V02     Ready  169.254.254.18   2020:0:0:1::212
```

To verify the RMI related ROMMON variables for both active and standby controllers, run the following command

```
Device# show romvar | i RMI

RMI_INTERFACE_NAME = Vlan52
RMI_CHASSIS_LOCAL_IPV6 = 2020:0:0:1::212
RMI_CHASSIS_REMOTE_IPV6 = 2020:0:0:1::211
```

Verifying Redundancy Port Interface Configuration

To verify the Redundancy Port Interface (RIF) resource status in an active instance, run the following command:

```
Device# show platform software rif-mgr chassis active R0 resource-status
RIF Resource Status

    RP Status             : Up
    RMI Status            : Up
    Current Chassis State : Active
    Peer Chassis State    : Standby
```

To verify the RIF resource status in a standby instance, run the following command:

```
Device# show platform software rif-mgr chassis standby R0 resource-status
RIF Resource Status

    RP Status             : Up
    RMI Status            : Up
    Current Chassis State : Standby
    Peer Chassis State    : Active
```

To verify the RMI link re-establishment count and the time since the RMI link is Up in the active instance, run the following command:

```
Device# show platform software rif-mgr chassis active R0 rmi-connection-details
RMI Connection Details
    RMI Link re-establish count : 2
    RMI Link Uptime             : 21 hours 8 minutes 43 seconds
    RMI Link Upsince            : 08/05/2021 13:46:01
```

To verify the RMI link re-establishment count and the time since the RMI link is Down in the active instance, run the following command:

```
Device# show platform software rif-mgr chassis active R0 rmi-connection-details
RMI Connection Details
    RMI Link re-establish count : 1
    RMI Link Downtime           : 28 seconds
    RMI Link Downsince          : 07/16/2021 03:19:11
```

To verify the RMI link re-establishment count and the time since the RMI link is Up in the standby instance, run the following command:

```
Device# show platform software rif-mgr chassis standby R0 rmi-connection-details
RMI Connection Details
    RMI Link re-establish count : 1
    RMI Link Uptime             : 1 hour 39 minute 9 seconds
    RMI Link Upsince            : 07/16/2021 01:31:41
```

To verify the RMI link re-establishment count and the time since the RMI link is Down in the standby instance, run the following command:

```
Device# show platform software rif-mgr chassis standby R0 rmi-connection-details
RMI Connection Details
    RMI Link re-establish count : 1
    RMI Link Downtime           : 22 seconds
    RMI Link Downsince          : 07/16/2021 03:19:17
```

To verify the RP link re-establishment count and the time since the RP link is UP for days in the active instance, run the following command:

```
Device# show platform software rif-mgr chassis active R0 rp-connection-details
RP Connection Details
    RP Connection Uptime  : 12 days 17 hours 1 minute 39 seconds
    RP Connection Upsince : 07/03/2021 07:06:20
```

To verify the RP link re-establishment count and the time since the RP link is Down in the active instance, run the following command:

```
Device# show platform software rif-mgr chassis active R0 rp-connection-details
RP Connection Details
    RP Connection Downtime     : 4 seconds
    RP Connection Downsince    : 07/16/2021 03:33:04
```

To verify the RP link re-establishment count and the time since the RP link is UP in the standby instance, run the following command:

```
Device# show platform software rif-mgr chassis standby R0 rp-connection-details
RP Connection Details
    RP Connection Uptime  : 12 days 17 hours 2 minutes 1 second
    RP Connection Upsince : 07/03/2021 07:05:58
```

To verify the RP link re-establishment count and the time since the RP link is Down in the standby instance, run the following command:

```
Device# show platform software rif-mgr chassis standby R0 rp-connection-details
RP Connection Details
```

```
    RP Connection Downtime    : 22 seconds
    RP Connection Downsince   : 07/16/2021 03:19:17
```

To verify the RIF and stack manager internal statistics in the active instance, run the following command:

```
Device# show platform software rif-mgr chassis active R0 rif-stk-internal-stats
RIF Stack Manager internal stats

    Stack-mgr reported RP down            : False
    DAD link status reported to Stack-Mgr : True
```

To verify the RIF and stack manager internal statistics in the standby instance, run the following command:

```
Device# show platform software rif-mgr chassis standby R0 rif-stk-internal-stats
RIF Stack Manager internal stats

    Stack-mgr reported RP down            : False
    DAD link status reported to Stack-Mgr : True
```

To verify the number of packets sent or received for each type in the active instance, run the following command:

```
Device# show platform software rif-mgr chassis active R0 lmp-statistics
LMP Statistics

Info Type Sent                    : 6
Solicit Info Type Sent            : 0
Unsolicit Info Type Sent          : 6
Reload Type Sent                  : 0
Recovery Type Sent                : 1
Gateway Info Type Sent            : 0
Enquiry Type Sent                 : 0
Solicit Enquiry Type Sent         : 0
Unsolicit Enquiry Type Sent       : 0

Info Type Received                : 5
Solicit Info Type Received        : 2
Unsolicit Info Type Received      : 3
Reload Type Received              : 0
Recovery Type Received            : 0
Gateway Info Type Received        : 4
Enquiry Type Received             : 0
Solicit Enquiry Type Received     : 0
Unsolicit Enquiry Type Received   : 0
```

To verify the number of packets sent or received for each type in the standby instance, run the following command:

```
Device# show platform software rif-mgr chassis standby R0 lmp-statistics
LMP Statistics

Info Type Sent                   : 6
Solicit Info Type Sent           : 0
Unsolicit Info Type Sent         : 6
Reload Type Sent                 : 0
Recovery Type Sent               : 0
Gateway Info Type Sent           : 4
Enquiry Type Sent                : 0
Solicit Enquiry Type Sent        : 0
Unsolicit Enquiry Type Sent      : 0

Info Type Received               : 5
Solicit Info Type Received       : 3
Unsolicit Info Type Received     : 2
Reload Type Received             : 0
Recovery Type Received           : 1
```

```
Gateway Info Type Received       : 0
Enquiry Type Received            : 0
Solicit Enquiry Type Received    : 0
Unsolicit Enquiry Type Received  : 0
```

Information About Auto-Upgrade

The Auto-Upgrade feature enables the standby controller to upgrade with the software image of the active controller so that both controllers form an HA pair.

Note

- This feature supports the active controller in INSTALL mode.
- This feature supports Cisco Catalyst 9800 Series Wireless Controller software versions 17.5.1 and later.
- This feature is triggered in the standby controller only when the active image is in committed state.

Use Cases

The following are the use cases and functionalities supported by the Auto-Upgrade feature:

- Handling software version mismatch: During an upgrade, if one of the redundancy port is upgraded to a newer version, and the other one is not upgraded at the same time, the active port tries to copy its packages to the other port using the Auto-Upgrade feature. You can enable Auto-Upgrade in this situation using configuration or by manually running the **software auto-upgrade enable** privileged EXEC command.

  The auto-upgrade configuration is enabled by default.

Note Auto-upgrade upgrades the mismatched redundancy port only when both the active redundancy port and the mismatched redundancy port are in INSTALL mode.

- HA pair: If one of the controller is not upgraded successfully, use Auto-Upgrade to upgrade the controller on the newly deployed HA pair, which can each be a different version.
- SMUs (APSP, APDP, and so on): If the SMUs that are successfully installed on the active controller when the standby controller was offline. In this scenario, when the standby controller comes up online, the Auto-Upgrade copies this SMU to the standby controller and installs it.

Configuration Workflow

#unique_1861

Configuring Auto-Upgrade (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**software auto-upgrade enable** **Example:** `Device(config)# software auto-upgrade enable`	Enables the Auto-Upgrade feature. (This feature is enabled by default.) If you disable this feature using the **no** form of this command, you need to manually auto upgrade using the **install autoupgrade** command in privileged EXEC mode.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Use Case for Link Layer Discovery Protocol (LLDP)

In a high-availability (HA) setup, when two wireless units act as active and standby, the LLDP still runs independently in both.

When you execute the LLDP neighbors command, the system name as the neighbor entry in the uplink switch is displayed as *hostname*-**stbdy**.

Enabling LLDP (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**lldp run** **Example:** `Device(config)# lldp run`	Enables Link Layer Discovery Protocol (LLDP).

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Enabling LLDP Timers (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**lldp holdtime** *time_in_secs* **Example:** `Device(config)# lldp holdtime 100`	Enables LLDP timers. The timer decides how long the receiver must keep the packet. Valid range is from 0 to 65535 seconds.
Step 3	**lldp reinit** *delay_in_secs* **Example:** `Device(config)# lldp reinit 3`	Specifies the delay, in seconds for LLDP to initialize. Valid range is from 2 to 5 seconds.
Step 4	**lldp timer** *time_in_secs* **Example:** `Device(config)# lldp timer 7`	Specifies the rate at which the LLDP packets are sent, in seconds. Valid range is from 5 to 65534 seconds.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Enabling LLDP TLV-Select (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**lldp tlv-select** [**mac-phy-cfg** | **management-address** | **port-description** |	Enables type, length, and value (TLV) selection for LLDP.

	Command or Action	Purpose
	port-vlan | **system-capabilities** | **system-description**] **Example:** `Device(config)# lldp tlv-select port-vlan`	• **mac-phy-cfg**: IEEE 802.3 MAC, physical configuration, or status TLV. • **management-address**: Management address TLV. • **port-description**: Port description TLV. • **port-vlan**: Port VLAN ID TLV. • **system-capabilities**: System capabilities TLV. • **system-description**: System description TLV.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying LLDP

Use the following **show** commands to view the LLDP details independently in the active and standby controller.

To verify the timer and status in the active and standby controller, use the following command:

```
Device# show lldp
Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

To verify the neighbor details in the active controller, use the following command:

```
Device# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
9500-SW             Tw0/0/0        120        B,R             Twe1/0/14
```

To verify the neighbor details in the standby controller, use the following command:

```
Device# show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
9500-SW             Tw0/0/0        120        B,R             Twe1/0/13
Total entries displayed: 1
```

To verify the LLDP neighbor (TLV) detail, use the following command:

```
Device# show lldp neighbors detail
------------------------------------------------
Local Intf: Te0/0/0
```

```
Chassis id: 2cd0.2d62.be80
Port id: Te1/1
Port Description: TenGigabitEthernet1/1
System Name: HSRP-ROUTER-1-15.cisco.com

System Description:
Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch  Software (cat4500e-UNIVERSAL-M),
 Version 03.09.00.E RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 19-Jul

Time remaining: 99 seconds
System Capabilities: B,R
Enabled Capabilities: B,R
Management Addresses:
    IP: 8.109.0.1
    IPV6: 2001:12:1::2
Auto Negotiation - not supported
Physical media capabilities:
    Other/unknown
Media Attachment Unit type - not advertised
Vlan ID: 109
Peer Source MAC: 2cd0.2d62.be80
```

To verify the LLDP details in the uplink switch, use the following command:

```
Device# show lldp neighbors detail
------------------------------------------------
Local Intf: Te1/1
Chassis id: d4e8.80b3.0420
Port id: Te0/0/0
Port Description: TenGigabitEthernet0/0/0
System Name: WLC-BGL15.cisco.com

System Description:
Cisco IOS Software [Bangalore], C9800 Software (C9800_IOSXE-K9), Experimental Version
17.9.20220630:200739
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Thu 30-Jun-22 13:19

Time remaining: 107 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses:
    IP: 8.109.0.47
    IPV6: FD09:8:109::45
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
Vlan ID: 109
```

To verify LLDP packet errors, use the following command:

```
Device# show lldp errors
LLDP errors/overflows:
Total memory allocation failures: 0
Total encapsulation failures: 0
Total input queue overflows: 0
Total table overflows: 0
```

To verify LLDP traffic statistics, use the following command:

```
Device# show lldp traffic
LLDP traffic statistics:
Total frames out: 18470
```

```
Total entries aged: 0
Total frames in: 6156
Total frames received in error: 0
Total frames discarded: 0
Total TLVs discarded: 0
Total TLVs unrecognized: 0
```

PART X

Quality of Service

- Quality of Service, on page 1511
- Wireless Auto-QoS, on page 1543
- Native Profiling, on page 1549
- Air Time Fairness, on page 1561
- IPv6 Non-AVC QoS Support, on page 1571
- QoS Basic Service Set Load, on page 1575

CHAPTER 139

Quality of Service

- Wireless QoS Overview, on page 1511
- Wireless QoS Targets, on page 1512
- Wireless QoS Mobility, on page 1513
- Precious Metal Policies for Wireless QoS, on page 1513
- Prerequisites for Wireless QoS, on page 1514
- Restrictions for QoS on Wireless Targets, on page 1514
- Metal Policy Format, on page 1515
- How to apply Bi-Directional Rate Limiting, on page 1522
- How to apply Per Client Bi-Directional Rate Limiting, on page 1529
- How to Configure Wireless QoS, on page 1534
- Configuring Custom QoS Mapping, on page 1538
- Configuring DSCP-to-User Priority Mapping Exception, on page 1539
- Configuring Trust Upstream DSCP Value, on page 1541

Wireless QoS Overview

Quality of Service (QoS), provides the ability to prioritize the traffic by giving preferential treatment to specific traffic over the other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput.

A target is the entity where the policy is applied. Wireless QoS policies for SSID and client are applied in the upstream and (or) downstream direction. The flow of traffic from a wired source to a wireless target is known as downstream traffic. The flow of traffic from a wireless source to a wired target is known as upstream traffic.

The following are some of the specific features provided by wireless QoS:

- SSID and client policies on wireless QoS targets
- Marking and Policing (also known as Rate Limiting) of wireless traffic
- Mobility support for QoS

Wireless QoS Targets

This section describes the various wireless QoS targets available on a device.

SSID Policies

You can create QoS policies on SSID in both the ingress and egress directions. If not configured, there is no SSID policy applied.

The policy is applicable per AP per SSID.

You can configure policing and marking policies on SSID.

Client Policies

Client policies are applicable in the ingress and egress direction. You can configure policing and marking policies on clients. AAA override is also supported.

Supported QoS Features on Wireless Targets

This table describes the various features available on wireless targets.

Table 106: QoS Features Available on Wireless Targets

Target	Features	Direction Where Policies Are Applicable
SSID	• Set • Police • Drop	Upstream and downstream
Client	• Set • Police • Drop	Upstream and downstream

This table describes the various features available on wireless targets.

Table 107: QoS Policy Actions

Policy Action Types	Wireless Target Support	
	Local Mode	Flex Mode
Police	Supported	Supported
Set	Supported	Supported

This table describes the various features available on wireless targets.

Table 108: QoS Policy Set Actions

Set Action Types	Supported	
	Local Mode	Flex Mode
set dscp	Supported	Supported
set qos-group	Supported	Not Supported
set wlan user-priority (downstream only)	Supported (BSSID only)	Supported (BSSID only)

Wireless QoS Mobility

Wireless QoS mobility enables you to configure QoS policies so that the network provides the same service anywhere in the network. A wireless client can roam from one location to another and as a result the client can get associated to different access points associated with a different device. Wireless client roaming can be classified into two types:

- Intra-device roaming
- Inter-device roaming

Note In a foreign WLC, client statistics are not displayed.

Note The client policies must be available on all of the devices in the mobility group. The same SSID policy must be applied to all devices in the mobility group so that the clients get consistent treatment.

Precious Metal Policies for Wireless QoS

The precious metal policies are system-defined policies that are available on the controller . They cannot be removed or changed.

The following policies are available:

- Platinum—Used for VoIP clients.
- Gold—Used for video clients.
- Silver— Used for traffic that can be considered best-effort.
- Bronze—Used for NRT traffic.

These policies are pre-configured. They cannot be modified.

For client metal policies, they can be pushed using AAA.

Based on the policies applied, the 802.11e (WMM), and DSCP fields in the packets are affected.

For more information about metal policies see the Metal Policy Map, on page 1515 section.

For more information about DSCP to UP mapping, see the #unique_1878 table.

Prerequisites for Wireless QoS

Before configuring wireless QoS, you must have a thorough understanding of these items:

- Wireless concepts and network topologies.
- Understanding of QoS implementation.
- Modular QoS CLI (MQC). For more information on Modular QoS, see the MQC guide
- The types of applications used and the traffic patterns on your network.
- Bandwidth requirements and speed of the network.

Restrictions for QoS on Wireless Targets

General Restrictions

A target is an entity where a policy is applied. A policy can be applied to a wireless target, which can be an SSID or client target, in the downstream and/or upstream direction. Downstream indicates that traffic is flowing from the controller to the wireless client. Upstream indicates that traffic is flowing from wireless client to the controller.

- Hierarchical (Parent policy and child policy) QoS is not supported.
- SSID and client targets can be configured only with marking and policing policies.
- One policy per target per direction is supported.
- Class maps in a policy map can have different types of filters. However, only one marking action (set dscp) is supported.
- Only one set action per class is supported.
- Access group matching is not supported.
- Access group (ACL) matching is not supported by access points in flex mode for local switching traffic.
- SIP Call Admission Control (CAC) is not supported on the central switching mode.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, SIP Call Admission Control (CAC) is not supported.
- Applying QoS on the WMI interface is not supported, as it may reboot the controller.

AP Side Restrictions

- In Cisco Embedded Wireless Controller, FlexConnect local switching, and SDA deployments, the QoS policies are enforced on the AP. Due to this AP-side restriction, police actions (e.g., rate limiting) are only enforced at a per flow (5-tuple) level and not per client.
- For FlexConnect local switching (local authentication) with AAA override enabled and external AAA server, only air space VLAN and ACL are supported as part of the AAA override and not the QoS override or other overrides.

Control Plane Rate Limiting and Policing

You need not explicitly configure control plane rate limiting or policing on the controller. The controller has embedded mechanisms (like policers) to protect the CPU by policing control plane traffic directed towards it. If you're migrating from AireOS to IOS-XE, this change is taken care of at the code level.

Metal Policy Format

Metal Policy Map

Table 109: Platinum (46)

policy-map platinum-up	policy-map platinum

class cm-dscp-non-std-set-1
  set dscp ef
Class cm-dscp-non-std-set-2
 	
  set dscp ef
Class cm-dscp-cs6
  set dscp ef
Class cm-dscp-cs7
  set dscp ef
class class-default
	class cm-dscp-non-std-set-1
	  set dscp ef
	Class cm-dscp-non-std-set-2
	
	  set dscp ef
	Class cm-dscp-cs6
	  set dscp ef
	Class cm-dscp-cs7
	  set dscp ef
	class class-default

Table 110: Gold (34)

policy-map gold-up	policy-map gold

class cm-dscp-non-std-set-1
  set dscp 34
Class cm-dscp-non-std-set-2
 	
  set dscp 34
Class cm-dscp-non-std-set-3
  set dscp 34
Class cm-dscp-cs5
  set dscp 34
Class cm-dscp-cs6
  set dscp 34
Class cm-dscp-cs7
  set dscp 34
Class cm-dscp-af4
  set dscp 34
Class cm-dscp-voice-admit
  set dscp 34
Class cm-dscp-ef
  set dscp 34
class class-default
	class cm-dscp-non-std-set-1
	  set dscp 34
	Class cm-dscp-non-std-set-2
	
	  set dscp 34
	Class cm-dscp-non-std-set-3
	  set dscp 34
	Class cm-dscp-cs5
	  set dscp 34
	Class cm-dscp-cs6
	  set dscp 34
	Class cm-dscp-cs7
	  set dscp 34
	Class cm-dscp-af4
	  set dscp 34
	Class cm-dscp-voice-admit
	  set dscp 34
	Class cm-dscp-ef
	  set dscp 34
	class class-default

Table 111: Silver (22)

policy-map silver-up	policy-map silver

class cm-dscp-non-std-set-1
  set dscp 22
Class cm-dscp-non-std-set-2
 	
  set dscp 22
Class cm-dscp-non-std-set-3
  set dscp 22
Class cm-dscp-non-std-set-4
 	
  set dscp 22
Class cm-dscp-cs3
  set dscp 22
Class cm-dscp-cs4
  set dscp 22
Class cm-dscp-cs5
  set dscp 22
Class cm-dscp-cs6
  set dscp 22
Class cm-dscp-cs7
 set dscp 22
Class cm-dscp-af3
  set dscp 22
Class cm-dscp-af4
  set dscp 22
Class cm-dscp-voice-admit
  set dscp 22
Class cm-dscp-ef
  set dscp 22
class class-default
	class cm-dscp-non-std-set-1
	  set dscp 22
	Class cm-dscp-non-std-set-2
	
	  set dscp 22
	Class cm-dscp-non-std-set-3
	  set dscp 22
	Class cm-dscp-non-std-set-4
	
	  set dscp 22
	Class cm-dscp-cs3
	  set dscp 22
	Class cm-dscp-cs4
	  set dscp 22
	Class cm-dscp-cs5
	  set dscp 22
	Class cm-dscp-cs6
	  set dscp 22
	Class cm-dscp-cs7
	 set dscp 22
	Class cm-dscp-af3
	  set dscp 22
	Class cm-dscp-af4
	  set dscp 22
	Class cm-dscp-voice-admit
	  set dscp 22
	Class cm-dscp-ef
	  set dscp 22
	class class-default

Table 112: Bronze (8)

policy-map bronze-up	policy-map bronze

class cm-dscp-non-std-set-1
  set dscp 8
Class cm-dscp-non-std-set-2
 	
  set dscp 8
Class cm-dscp-non-std-set-3
  set dscp 8
Class cm-dscp-non-std-set-4
 	
  set dscp 8
class cm-dscp-non-std-set-5
  set dscp 8
Class cm-dscp-cs1-7
  set dscp 8
class cm-dscp-af1
  set dscp 8
class cm-dscp-af2
  set dscp 8
Class cm-dscp-af3
  set dscp 8
Class cm-dscp-af4
  set dscp 8
Class cm-dscp-voice-admit
  set dscp 8
Class cm-dscp-ef
  set dscp 8
Class class-default
	class cm-dscp-non-std-set-1
	  set dscp 8
	Class cm-dscp-non-std-set-2
	
	  set dscp 8
	Class cm-dscp-non-std-set-3
	  set dscp 8
	Class cm-dscp-non-std-set-4
	
	  set dscp 8
	class cm-dscp-non-std-set-5
	  set dscp 8
	Class cm-dscp-cs1-7
	  set dscp 8
	class cm-dscp-af1
	  set dscp 8
	class cm-dscp-af2
	  set dscp 8
	Class cm-dscp-af3
	  set dscp 8
	Class cm-dscp-af4
	  set dscp 8
	Class cm-dscp-voice-admit
	  set dscp 8
	Class cm-dscp-ef
	  set dscp 8
	Class class-default

Class Maps

```
class-map match-any cm-dscp-non-std-set-1
match dscp 47  49  50  51  52  53  54 55

Class-map match-any cm-dscp-non-std-set-2
match dscp 57  58  59  60  61  62 63

class-map match-any cm-dscp-non-std-set-3
match dscp 35 37 39 41 42 43 45

class-map match-any cm-dscp-non-std-set-4
match dscp 23 25 27 29 31 33

class-map match-any cm-dscp-non-std-set-5
match dscp  9  11  13  15 17  19  21

Class-map match-any cm-dscp-cs2
match dscp 16

Class-map match-any cm-dscp-cs3
match dscp 24

Class-map match-any cm-dscp-cs4
match dscp 32

Class-map match-any cm-dscp-cs5
match dscp 40
Class-map match-any cm-dscp-cs6
```

```
match dscp 48

Class-map match-any cm-dscp-cs7
match dscp 56

Class-map match-any cm-dscp-af1
match dscp 10 12 14

Class-map match-any cm-dscp-af2
match dscp 18 20 22

Class-map match-any cm-dscp-af3
match dscp 26 28 30

Class-map match-any cm-dscp-af4
match dscp 34 36 38

Class-map match-any cm-dscp-voice-admit
match dscp 44

Class-map match-any cm-dscp-ef
match dscp 46

Class-map match-any cm-dscp-cs1-7
match dscp 8 16 24 32 40 48 56
```

DSCP to UP Mapping for Downstream Traffic

```
[0]->0 [1]->0 [2]->0 [3]->0 [4]->0 [5]->0 [6]->0 [7]->0
[8]->1 [9]->0 [10]->2 [11]->0 [12]->2 [13]->0 [14]->2 [15]->0
[16]->0 [17]->0 [18]->3 [19]->0 [20]->3 [21]->0 [22]->3 [23]->0
[24]->4 [25]->0 [26]->4 [27]->0 [28]->4 [29]->0 [30]->4 [31]->0
[32]->5 [33]->0 [34]->4 [35]->0 [36]->4 [37]->0 [38]->4 [39]->0
[40]->5 [41]->0 [42]->0 [43]->0 [44]->6 [45]->0 [46]->6 [47]->0
[48]->0 [49]->0 [50]->0 [51]->0 [52]->0 [53]->0 [54]->0 [55]->0
[56]->0 [57]->0 [58]->0 [59]->0 [60]->0 [61]->0 [62]->0 [63]->0
```

UP to DSCP Mapping for Upstream traffic

```
[0]->0 [1]->8 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->0
```

Auto QoS Policy Format

Policy Name	Policy-map Format	Class-map Format
enterprise-avc	policy-map AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy class AutoQos-4.0-wlan-Voip-Data-Class set dscp ef class AutoQos-4.0-wlan-Voip-Signal-Class set dscp cs3 class AutoQos-4.0-wlan-Multimedia-Conf-Class set dscp af41 class AutoQos-4.0-wlan-Transaction-Class set dscp af21 class AutoQos-4.0-wlan-Bulk-Data-Class set dscp af11 class AutoQos-4.0-wlan-Scavanger-Class set dscp cs1 class class-default set dscp default policy-map AutoQos-4.0-wlan-ET-SSID-Output-Policy class AutoQos-4.0-RT1-Class set dscp ef class AutoQos-4.0-RT2-Class set dscp af31 class class-default	

Policy Name	Policy-map Format	Class-map Format
		class-map match-any AutoQos-4.0-wlan-Voip-Data-Class match dscp ef class-map match-any AutoQos-4.0-wlan-Voip-Signal-Class match protocol skinny match protocol cisco-jabber-control match protocol sip match protocol sip-tls class-map match-any AutoQos-4.0-wlan-Multimedia-Conf-Class match protocol cisco-phone-video match protocol cisco-jabber-video match protocol ms-lync-video match protocol webex-media class-map match-any AutoQos-4.0-wlan-Transaction-Class match protocol cisco-jabber-im match protocol ms-office-web-apps match protocol salesforce match protocol sap class-map match-any AutoQos-4.0-wlan-Bulk-Data-Class match protocol ftp match protocol ftp-data match protocol ftps-data match protocol cifs class-map match-any AutoQos-4.0-wlan-Scavanger-Class match protocol netflix match protocol youtube match protocol skype match protocol bittorrent class-map match-any AutoQos-4.0-RT1-Class match dscp ef

Policy Name	Policy-map Format	Class-map Format
		match dscp cs6 class-map match-any AutoQos-4.0-RT2-Class match dscp cs4 match dscp cs3 match dscp af41
voice	policy-map platinum-up class dscp-for-up-4 set dscp 34 class dscp-for-up-5 set dscp 34 class dscp-for-up-6 set dscp 46 class dscp-for-up-7 set dscp 46 policy-map platinum class cm-dscp-34 set dscp 34 class cm-dscp-46 set dscp 46	
guest	Policy Map AutoQos-4.0-wlan-GT-SSID-Output-Policy Class class-default set dscp default Policy Map AutoQos-4.0-wlan-GT-SSID-Input-Policy Class class-default set dscp default	
port (only applies to Local Mode)	policy-map AutoQos-4.0-wlan-Port-Output-Policy class AutoQos-4.0-Output-CAPWAP-C-Class priority level 1 class AutoQos-4.0-Output-Voice-Class priority level 2 class class-default ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C permit udp any eq 5246 16666 any	class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C class-map match-any AutoQos-4.0-Output-Voice-Class match dscp ef

Architecture for Voice, Video and Integrated Data (AVVID)

IETF DiffServ Service Class	DSCP	IEEE 802.11e	
		User Priority	Access Category
Network Control	CS7	0	AC_BE (based on configuration)
Network Control	CS6	0	AC_BE (based on configuration)
Telephony	EF	6	AC_VO
VOICE-ADMIT	44	6	AC_VO

IETF DiffServ Service Class	DSCP	IEEE 802.11e	
		User Priority	Access Category
Signaling	CS5	5	AC_VI
Multimedia Conferencing	AF41 AF42 AF43	4	AC_VI
Real-Time Interactive	CS4	5	AC_VI
Multimedia Streaming	AF31 AF32 AF33	4	AC_VI
Broadcast Video	CS3	4	AC_VI
Low-Latency Data	AF21 AF22 AF23	3	AC_BE
OAM	CS2	0	AC_BE
High-Throughput Data	AF11 AF12 AF13	2	AC_BK
Standard	DF	0	AC_BE
Low-Priority Data	CS1	1	AC_BK
Remaining	Remaining	0	

How to apply Bi-Directional Rate Limiting

Information about Bi-Directional Rate Limiting

Bi-Directional Rate Limiting (BDRL) feature defines rate limits on both upstream and downstream traffic. These rate limits are individually configured. The rate limits can be configured on WLAN directly instead of QoS profiles, which will override QoS profile values. The WLAN rate limiting will always supersede Global QoS setting for controller and clients.

BDRL feature defines throughput limits for clients on their wireless networks and allows setting a priority service to a particular set of clients.

The following four QoS profiles are available to configure the rate limits:

- Gold
- Platinum
- Silver
- Bronze

The QoS profile is applied to all clients on the associated SSID. Therefore all clients connected to the same SSID will have the same rate limits.

To configure BDRL, select the QoS profile and configure the various rate limiting parameters. When rate limiting parameters are set to *0*, the rate limiting feature is not functional. Each WLAN has a QoS profile associated with it in addition to the configuration in the QoS profile.

Note BDRL in a mobility Anchor-Foreign setup must be configured both on Anchor and Foreign controller. As a best practice, it is recommended to perform identical configuration on both the controllers to avoid breakage of any feature.

BDRL is supported on Guest anchor scenarios. The feature is supported on IRCM guest scenarios with AireOS as Guest anchor or Guest Foreign. Cisco Catalyst 9800 Series Wireless Controller uses **Policing** option to rate limit the traffic.

To apply metal policy with BDRL, perform the following tasks:

- Configure Metal Policy on SSID
- Configure Metal Policy on Client
- #unique_1888
- #unique_1889
- #unique_1890
- #unique_1891

Prerequisites for Bi-Directional Rate Limiting

- Client metal policy is applied through AAA-override.
- You must specify the metal policy on ISE server.
- AAA-override must be enabled on policy profile.

Configure Metal Policy on SSID

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile1`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets platinum policy for input.
Step 5	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets platinum policy for output.

Configure Metal Policy on Client

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:**	Adds a user defined description to the new wireless policy.

	Command or Action	Purpose
	`Device(config-wireless-policy)# description profile with aaa override`	
Step 4	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Enables AAA override on the WLAN. **Note** After AAA-override is enabled and ISE server starts sending policy, client policy defined in service-policy client will not take effect.

Configure Bi-Directional Rate Limiting for All Traffic

Use the police action in the policy-map to configure BDRL.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map* **Example:** `Device(config)# policy-map policy-sample 1`	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-default`	Associates a class map with the policy map, and enters policy-map class configuration mode.
Step 4	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.

Configure Bi-Directional Rate Limiting Based on Traffic Classification

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**policy-map** *policy-map* **Example:** `Device(config)# policy-map policy-sample2`	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-sample-youtube`	Associates a class map with the policy map, and enters policy-map class configuration mode.
Step 4	**police** *rate* **Example:** `Device(config-pmap-c)# police 1000000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.
Step 5	**conform-action drop** **Example:** `Device(config-pmap-c-police)# conform-action drop`	Specifies the drop action to take on packets that conform to the rate limit.
Step 6	**exceed-action drop** **Example:** `Device(config-pmap-c-police)# exceed-action drop`	Specifies the drop action to take on packets that exceeds the rate limit.
Step 7	**exit** **Example:** `Device(config-pmap-c-police)# exit`	Exits the policy-map class configuration mode.
Step 8	**set dscp default** **Example:** `Device(config-pmap-c)# set dscp default`	Sets the DSCP value to default.
Step 9	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.
Step 10	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits the policy-map class configuration mode.
Step 11	**exit** **Example:** `Device(config-pmap)# exit`	Exits the policy-map configuration mode.

	Command or Action	Purpose
Step 12	**class-map match-any** *class-map-name* **Example:** `Device(config)# class-map match-any class-sample-youtube`	Selects a class map.
Step 13	**match protocol** *protocol* **Example:** `Device(config-cmap)# match protocol youtube`	Configures the match criteria for a class map on the basis of the specified protocol.

Apply Bi-Directional Rate Limiting Policy Map to Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile3`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile3`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy client input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy client input platinum-up`	Sets the input client service policy as platinum.
Step 5	**service-policy client output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy client output platinum`	Sets the output client service policy as platinum.
Step 6	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets the input service policy as platinum.

	Command or Action	Purpose
Step 7	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets the output service policy as platinum.

Apply Metal Policy with Bi-Directional Rate Limiting

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile3`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile3`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy client input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy client input platinum-up`	Sets the input client service policy as platinum.
Step 5	**service-policy client output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy client output platinum`	Sets the output client service policy as platinum.
Step 6	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets the input service policy as platinum.
Step 7	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets the output service policy as platinum.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Device(config-wireless-policy)# exit`	Exits the policy configuration mode.
Step 9	**policy-map** *policy-map* **Example:** `Device(config)# policy-map policy-sample 1`	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 10	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-default`	Associates a class map with the policy map, and enters configuration mode for the specified system class.
Step 11	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.

How to apply Per Client Bi-Directional Rate Limiting

Information About Per Client Bi-Directional Rate Limiting

The Per Client Bi-Directional Rate Limiting feature adds bi-directional rate limiting for each wireless clients on 802.11ac Wave 2 APs in a Flex local switching configuration. Earlier, the Wave 2 APs supported only per-flow rate limiting for a wireless client. When wireless client starts multiple streams of traffic, the client-based rate limiting does not work as expected. This limitation is addressed by this feature.

For instance, if the controller is configured with QoS policy and you expect each client to have a rate limiting cap of 1000 kbps. Due to per-flow rate limiting on the AP, if the wireless client starts a Youtube stream and FTP stream, each of them will be rate limited at 1000 Kbps, therefore the client will be 2000 Kbps rates. This is not desirable.

Use Cases

The following are the use cases supported by the Per Client Bi-Directional Rate Limiting feature:

Use Case -1

Configuring only default class map

If policy map is configured only with default class map and mapped only to QoS client policy, AP does a per client rate limit to the client connected to AP.

Use Case-2

Changing from per client rate limit to per flow rate limit

If policy map is configured with another different class map along with a default class map and mapped to QoS client policy, AP performs per flow rate limit to client. As policy map has different class map along with the default class map. The per client rate limit values are cleared, if the AP has previously configured per client rate limit.

If the policy map has more than one class map, then additional class map is configured along with the default class map. So, the rate limit is applied from per client to per flow. The per client rate limit value is deleted from the rate info token bucket.

Use Case-3

Changing from per flow rate limit to per client limit

If different class map is removed from policy map and policy map has only one default class map, AP performs a per client rate limit to client.

The following covers the high-level steps for Per Client Bi-Directional Rate Limiting feature:

1. Configure a policy map to WLAN through policy profile.
2. Map the QoS related policy map to WLAN.
3. Configure policy map with the default class map.
4. Configure different police rate value for class Default map.

Note If policy map has class Default with valid police rate value, AP applies that rate limit to the overall client data traffic flow.

5. Apply the policy map with class Default to QoS client policy in WLAN policy profile.

Prerequisites for Per Client Bi-Directional Rate Limiting

- This feature is exclusive to QoS client policy, that is, the policy profile must have only QoS Policy or policy target as client.
- If policy map has class default with valid police rate value, AP applies that rate limit value to the overall client data traffic flow.

Restrictions on Per Client Bi-Directional Rate Limiting

- If policy map has class map other than the class Default map, the per client rate limit does not work in AP.
- From Cisco IOS XE Bengaluru 17.5.x onwards, AAA override can be leveraged to push the attributes to achieve per client rate limit.
- From Cisco IOS XE Bengaluru 17.6 onwards, per client bi-directional rate limit is supported on 802.11ac Wave 2 APs and 11ax APs in the Flex local switching configuration. However, due to the CSCwh74415 defect, in order to avoid the latest QoS policy return (which needs to be applied to all the clients connected to the same AP, thereby overriding all other QoS policies), you must add the AV-pairs in the authorization profile on Cisco ISE.

Configuring Per Client Bi-Directional Rate Limiting (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name.

The **Edit Policy Profile** window is displayed.

Note The **Edit Policy Profile** window is displayed and configured in default class map only.

Step 3 Choose the **QOS And AVC** tab.

Step 4 In the **QoS Client Policy** settings, choose the policies from the **Egress** and **Ingress** drop-down lists.

Note You need to apply the default policy map to the QoS Client Policy.

Step 5 Click **Update & Apply to Device**.

Verifying Per Client Bi-Directional Rate Limiting

To verify whether per client is applied in AP, use the following command:

```
Device# show rate-limit client
Config:
            mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in
 nrt_burst_out nrt_burst_in
A0:D3:7A:12:6C:5E   0           0          0            0           0            0
   0            0            0
Statistics:
            name     up down
        Unshaped      0    0
  Client RT pass 697610 8200
 Client NRT pass      0    0
 Client RT drops      0    0
Client NRT drops      0   16
              9    180    0
Per client rate limit:
             mac vap rate_out rate_in            policy
A0:D3:7A:12:6C:5E   0       88      23 per_client_rate_2
```

Configuring BDRL Using AAA Override

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile policy** *profile-name* **Example:** `Device (config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa`	Configures AAA override to apply policies coming from the AAA server or ISE the Cisco Identify Services Engine (ISE) server. The following attributes are available in the RADIUS server: • Airespace-Data-Bandwidth-Average-Contract: 8001 • Airespace-Real-Time-Bandwidth-Average-Contract: 8002 • Airespace-Data-Bandwidth-Burst-Contract: 8003 • Airespace-Real-Time-Bandwidth-Burst-Contract: 8004 • Airespace-Data-Bandwidth-Average-Contract-Upstream: 8005 • Airespace-Real-Time-Bandwidth-Average-Contract-Upstream: 8006 • Airespace-Data-Bandwidth-Burst-Contract-Upstream: 8007 • Airespace-Real-Time-Bandwidth-Burst-Contract-Upstream: 8008 **Note** 8001, 8002, 8003, 8004, 8005, 8006, 8007, and 8008 are the desired rate-limit values configured as an example.

Verifying Bi-Directional Rate-Limit

To verify the bi-directional rate limit, use the following command:

```
Device# show wireless client mac-address E8-8E-00-00-00-71 detailClient MAC Address :
e88e.0000.0071
Client MAC Type     : Universally Administered Address
Client IPv4 Address : 100.0.7.94
Client Username     : e88e00000071
AP MAC Address      : 0a0b.0c00.0200
AP Name             : AP6B8B4567-0002
AP slot             : 0
```

```
Client State        : Associated
Policy Profile      : dnas_qos_profile_policy
Flex Profile        : N/A
Wireless LAN Id     : 10
WLAN Profile Name   : QoS_wlan
Wireless LAN Network Name (SSID): QoS_wlan
BSSID : 0a0b.0c00.0200
Connected For       : 28 seconds
Protocol            : 802.11n - 2.4 GHz
Channel             : 1
Client IIF-ID       : 0xa0000034
Association Id      : 10
Authentication Algorithm : Open System
Idle state timeout  : N/A
Session Timeout     : 1800 sec (Remaining time: 1777 sec)
Session Warning Time : Timer not running
Input Policy Name    : None
Input Policy State   : None
Input Policy Source  : None
Output Policy Name   : None
Output Policy State  : None
Output Policy Source : None
WMM Support          : Enabled
U-APSD Support       : Disabled
Fastlane Support     : Disabled
Client Active State  : In-Active
Power Save           : OFF
Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 8005 (kbps)
  QoS Realtime Average Data Rate Upstream    : 8006 (kbps)
  QoS Burst Data Rate Upstream               : 8007 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 8008 (kbps)
  QoS Average Data Rate Downstream           : 8001 (kbps)
  QoS Realtime Average Data Rate Downstream  : 8002 (kbps)
  QoS Burst Data Rate Downstream             : 80300 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 8004 (kbps)
```

To verify the rate-limit details from the AP terminal, use the following command

```
Device# show rate-limit client
Config:
mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst_out
 nrt_burst_in
00:1C:F1:09:85:E7 0 8001 8002 8003 8004 8005 8006 8007 8008
Statistics:
name up down
Unshaped 0 0
Client RT pass 0 0
Client NRT pass 0 0
Client RT drops 0 0
Client NRT drops 0 0
Per client rate limit:
mac vap rate_out rate_in policy
```

How to Configure Wireless QoS

Configuring a Policy Map with Class Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **QoS**.

Step 2 Click **Add** to view the **Add QoS** window.

Step 3 In the text box next to the **Policy Name**, enter the name of the new policy map that is being added.

Step 4 Click **Add Class-Maps**.

Step 5 Configure **AVC** based policies or **User Defined** policies. To enable **AVC** based policies, and configure the following:

a) Choose either **Match Any** or **Match All**.

b) Choose the required **Mark Type**. If you choose **DSCP** or **User Priority**, you must specify the appropriate **Mark Value**.

c) Check the **Drop** check box to drop traffic from specific sources.

Note When **Drop** is enabled, the **Mark Type** and **Police(kbps)** options are disabled.

d) Based on the chosen **Match Type**, select the required protocols from the **Available Protocol(s)** list and move them to the **Selected Protocol(s)** list. These selected protocols are the ones from which traffic is dropped.

e) Click **Save**.

Note To add more Class Maps, repeat steps 4 and 5.

Step 6 To enable **User-Defined** QoS policy, and the configure the following:

a) Choose either **Match Any** or **Match All**.

b) Choose either **ACL** or **DSCP** as the **Match Type** from the drop-down list, and then specify the appropriate **Match Value**.

c) Choose the required **Mark Type** to associate with the mark label. If you choose *DSCP*, you must specify an appropriate **Mark Value**.

d) Check the **Drop** check box to drop traffic from specific sources.

Note When **Drop** is enabled, the **Mark Type** and **Police(kbps)** options are disabled.

e) Click **Save**.

Note To define actions for all the remaining traffic, in the Class Default, choose **Mark** and/or **Police(kbps)** accordingly.

Step 7 Click **Save & Apply to Device**.

Configuring a Class Map (CLI)

Follow the procedure given below to configure class maps for voice and video traffic:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class-map** *class-map-name* **Example:** `Device(config)# class-map test`	Creates a class map.
Step 3	**match dscp** *dscp-value* **Example:** `Device(config-cmap)# match dscp 46`	Matches the DSCP value in the IPv4 and IPv6 packets. **Note** By default for the class map the value is match-all.
Step 4	**end** **Example:** `Device(config-cmap)# end`	Exits the class map configuration and returns to the privileged EXEC mode.
Step 5	**show class-map** *class-map-name* **Example:** `Device# show class-map class_map_name`	Verifies the class map details.

Configuring Policy Profile to Apply QoS Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click the name of the policy profile.

Step 3 In the **Edit Policy Profile** window, click the **QoS and AVC** tab.

Step 4 Under **QoS SSID Policy**, choose the appropriate **Ingress** and **Egress** policies for WLANs.

Note The ingress policies can be differentiated from the egress policies by the suffix *-up*. For example, the Platinum ingress policy is named *platinum-up*.

Step 5 Under **QoS Client Policy**, choose the appropriate **Ingress** and **Egress** policies for clients.

Step 6 Click **Update & Apply to Device**.

Note Only custom policies are displayed under **QoS Client Policy**. AutoQoS policies are auto generated and not displayed for user selection.

Configuring Policy Profile to Apply QoS Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy qostest`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**service-policy client** {**input** | **output**} *policy-name* **Example:** `Device(config-wireless-policy)# service-policy client input policy-map-client`	Applies the policy. The following options are available. • **input**—Assigns the client policy for ingress direction on the policy profile. • **output**—Assigns the client policy for egress direction on the policy profile.
Step 4	**service-policy** {**input** | **output**} *policy-name* **Example:** `Device(config-wireless-policy)# service-policy input policy-map-ssid`	Applies the policy to the BSSID. The following options are available. • **input**—Assigns the policy-map to all clients in WLAN. • **output**—Assigns the policy-map to all clients in WLAN.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.

Applying Policy Profile to Policy Tag (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page in the **Policy** tab, click **Add**.

Step 3 In the **Add Policy Tag** window that is displayed, enter a name and description for the policy tag.

Step 4 Map the required WLAN IDs and WLAN profiles with appropriate policy profiles.

Step 5 Click **Update & Apply to Device**.

Applying Policy Profile to Policy Tag (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy qostag`	Configures policy tag and enters the policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan test policy qostest`	Maps a policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
Step 5	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	Displays the configured policy tags. **Note** To view the detailed information of a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Attaching Policy Tag to an AP

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters the ap profile configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag qostag`	Maps a Policy tag to the AP.
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
Step 5	**show ap tag summary** **Example:** `Device# show ap tag summary`	Displays the ap details and tags associated to it.

Configuring Custom QoS Mapping

For interworking with IP networks, a map is devised between the 802.11e user priorities and the IP differentiated services code point (DSCP). Enable Hotspot 2.0 on the WLAN to support mapping exception.

Note Custom QoS mapping only applies to Hotspot 2.0.

Mapping is specified as DSCP ranges to individual user priority values, and as a set of exceptions with one-to-one mapping between DSCP values and UP values. If a QoS map is enabled and user-configurable mappings are not added, the default values are used.

Note Egress = Downstream = Output and Ingress = Upstream = Input

The following table shows a QoS map, where an AP provides a wireless client with the required mapping from IP DSCP to 802.11e user priority.

Table 113: Default DSCP-Range-to-User Priority Mapping

IP DSCP Range	802.11e User Priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile hs2-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**qos-map dscp-to-up-range** *user-priority up-to-dscp dscp-start dscp-end* **Example:** `Device(config-ap-profile)# qos-map dscp-to-up-range 6 52 23 62`	Configures DSCP-to-user priority mapping. You can configure up to eight configuration entries; one for each *user-priority* value. If you do not configure a custom value, a non-configured value (0xFF) is sent to the AP. Use the **no** form of this command to disable the configuration. To delete all the custom mappings, use the **no dscp-to-up-range** command.

Configuring DSCP-to-User Priority Mapping Exception

When you configure a QoS mapping or exception, a custom QoS map is created and sent to the corresponding AP.

If there are no DSCP-to-user priority mapping or exception entries, an empty QoS map is used.

The following table shows the set of exceptions with one-to-one mapping between DSCP values and user priority values.

Table 114: Default DSCP-Range-to-User Priority Mapping Exceptions

IP DSCP	802.11e User Priority
0	0
2	1
4	1
6	1
10	2
12	2
14	2
18	3
20	3
22	3
26	4
34	5
46	6
48	7
56	7

Note Voice admission control should be disabled for user priorites 6 and 7, from the controller GUI. To disable **Admission Control (ACM)**, choose **Configuration** > **Radio Configurations** > **Media Parameters**.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile hs2-profile`	Configures an AP profile and enters AP profile configuration mode.

	Command or Action	Purpose
Step 3	**qos-map dscp-to-up-exception** *dscp-num user-priority* **Example:** `Device(config-ap-profile)# qos-map dscp-to-up-exception 42 6`	Configures DSCP-to-user priority exception.

Configuring Trust Upstream DSCP Value

The controller marks the 802.11 user priority value in Traffic Identifier (TID) field based on the DSCP value in IP header.

Note The AP forwards the DSCP value to Air, if 802.11 user priority value is set.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile hs2-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**qos-map trust-dscp-upstream** **Example:** `Device(config-ap-profile)# qos-map trust-dscp-upstream`	Configures the AP to trust upstream DSCP instead of user priority. Use the **no** form of the command to disable the configuration. **Note** From the Cisco IOS XE 17.4.x release onwards, the **qos-map trust-dscp-upstream** is the default setting so that client DSCP is, by default, maintained end to end. **Note** When the **trust-dscp-upstream** command is enabled, the value of DSCP is 18. Silver is the default if nothing is configured.

CHAPTER 140

Wireless Auto-QoS

•
• Information About Auto QoS, on page 1543
• How to Configure Wireless AutoQoS, on page 1544

Information About Auto QoS

Wireless Auto QoS automates deployment of wireless QoS features. It has a set of predefined profiles which can be further modified by the customer to prioritize different traffic flows. Auto-QoS matches traffic and assigns each matched packet to qos-groups. This allows the output policy map to put specific qos-groups into specific queues, including into the priority queue.

AutoQoS Policy Configuration

Table 115: AutoQoS Policy Configuration

Mode	Client Ingress	Client Egress	BSSID Ingress	BSSID Egress	Port Ingress	Port Egress	Radio
Voice	N/A	N/A	P3	P4	N/A	P7	ACM on
Guest	N/A	N/A	P5	P6	N/A	P7	
Fastlane	N/A	N/A	N/A	N/A	N/A	P7	edca-parameters fastlane
Enterprise-avc	N/A	N/A	P1	P2	N/A	P7	

P1	AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy
P2	AutoQos-4.0-wlan-ET-SSID-Output-Policy
P3	platinum-up
P4	platinum
P5	AutoQos-4.0-wlan-GT-SSID-Input-Policy

P6	AutoQos-4.0-wlan-GT-SSID-Output-Policy
P7	AutoQos-4.0-wlan-Port-Output-Policy

How to Configure Wireless AutoQoS

Configuring Wireless AutoQoS on Profile Policy

You can enable AutoQoS on a profile policy.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**wireless autoqos policy-profile** *policy-name* **mode { enterprise-avc | fastlane | guest | voice}** **Example:** `Device# wireless autoqos policy-profile test-profile mode voice`	Configures AutoQoS wireless policy. • **enterprise-avc**—Enables AutoQoS Wireless Enterprise AVC Policy. • **fastlane**—Enable AutoQoS Wireless Fastlane Policy. • **guest**—Enable AutoQoS Wireless Guest Policy. • **voice**—Enable AutoQoS Wireless Voice Policy. **Note** AutoQoS MIB attribute does not support full functionality with service policy. Service policy must be configured manually. Currently, there is only support for AutoQoS mode.

What to do next

Note After enabling AutoQoS, we recommend that you wait for a few seconds for the policy to install and then try and modify the AutoQoS policy maps if required; or retry if the modification is rejected.

Disabling Wireless AutoQoS

To globally disable Wireless AutoQoS:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**shutdown** **Example:** `Device# shutdown`	Shuts down the policy profile.
Step 3	**wireless autoqos disable** **Example:** `Device# wireless autoqos disable`	Globally disables wireless AutoQoS.
Step 4	**[no] shutdown** **Example:** `Device# no shutdown`	Enables the wireless policy profile. **Note** Disabling Auto QoS does not reset global radio configurations like CAC and EDCA parameters.

Rollback AutoQoS Configuration (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **QoS**.
Step 2 Click **Disable AutoQoS**.
Step 3 Click **Yes** to confirm.

Rollback AutoQoS Configuration

Before you begin

Note AutoQoS MIB attribute does not support the full functionality with service policy. Currently, there is only support for AutoQoS mode. Service policy must be configured manually.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**clear platform software autoqos config template { enterprise_avc | guest}** **Example:** `Device# clear platform software autoqos config template guest`	Resets AutoQoS configuration. • enterprise-avc—Resets AutoQoS Enterprise AVC Policy Template. • guest—Resets AutoQoS Guest Policy Template.

Clearing Wireless AutoQoS Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Click on the **Policy Profile Name**.
Step 3 Go to **QOS and AVC** tab.
Step 4 From the **Auto Qos** drop-down list, choose **None**.
Step 5 Click **Update & Apply to Device**.

Clearing Wireless AutoQoS Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**shutdown** **Example:** `Device# shutdown`	Shuts down the policy profile.
Step 3	**wireless autoqos policy-profile** *policy-name* **mode clear** **Example:**	Clears the configured AutoQoS wireless policy.

	Command or Action	Purpose
	`Device# wireless autoqos policy-profile test-profile mode clear`	
Step 4	**[no] shutdown** **Example:** `no shutdown`	Enables the wireless policy profile.

Viewing AutoQoS on policy profile

Before you begin

AutoQoS is supported on the local mode and flex mode. AutoQoS configures a set of policies and radio configurations depending on the template. It is possible to override the service-policy that is configured by AutoQoS. The latest configuration takes effect, with AAA override policy being of highest priority.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Deviceenable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show wireless profile policy detailed** *policy-profile-name* **Example:** `Device# show wireless profile policy detailed testqos`	Shows policy-profile detailed parameters.

CHAPTER 141

Native Profiling

- Information About Native Profiling, on page 1549
- Creating a Class Map (GUI), on page 1550
- Creating a Class Map (CLI), on page 1551
- Creating a Service Template (GUI), on page 1553
- Creating a Service Template (CLI), on page 1554
- Creating a Parameter Map, on page 1555
- Creating a Policy Map (GUI), on page 1555
- Creating a Policy Map (CLI), on page 1556
- Configuring Native Profiling in Local Mode, on page 1558
- Verifying Native Profile Configuration, on page 1558

Information About Native Profiling

You can profile devices based on HTTP and DHCP to identify the end devices on the network. You can configure device-based policies and enforce these policies per user or per device policy on the network.

Policies allow profiling of mobile devices and basic onboarding of the profiled devices to a specific VLAN. They also assign ACL and QoS or configure session timeouts.

The policies are defined based on the following attributes:

- User group or user role
- Device type such as Windows clients, smartphones, tablets, and so on
- Service Set Identifier (SSID)
- Location, based on the access point group that the end point is connected to
- Time of the day
- Extensible Authentication Protocol (EAP) type, to check what EAP method that the client is getting connected to

When a wireless client joins an access point, certain QoS policies get enforced on the access point. One such feature is the native profiling for both upstream and downstream traffic at AP. The native profiling feature when clubbed with AAA override supports specific set of policies based on the time of day and day of week. The AAA override then applies these policies coming from a RADIUS server to the access point.

Let's consider a use case of time of the day in conjunction with user role. Usually, the user role is used as an extra matching criteria along with the time of day. You can club the time of day usage with any matching criteria to get the desired result. The matching will be performed when the client joins the controller .

You can configure policies as two separate components:

- Defining policy attributes as service templates that are specific to clients joining the network and applying policy match criteria
- Applying match criteria to the policy.

Note Before proceeding with the native profile configuration, ensure that HTTP Profiling and DHCP Profiling are enabled.

Note Native profiling is not supported with FlexConnect Local Authentication and Local Switching. Hence, do not configure **no central switching**, **no central authentication**, and **subscriber-policy-name** *name* commands together. ISSU will fail for this type of configuration. Ensure that you remove the configuration before attempting ISSU.

To configure Native Profiling, use one of the following procedures:

- Create a service template
- Create a class map

Note You can apply a service template using either a class map or parameter map.

- Create a parameter-map and associate the service template to parameter-map
  - Create a policy map
    1. If class-map has to be used: Associate the class-map to the policy-map and associate the service-template to the class-map.
    2. If parameter-map has to be used: Associate the parameter-map to the policy-map
  - Associate the policy-map to the policy profile.

Creating a Class Map (GUI)

Procedure

Step 1 Click **Configuration** > **Services** > **QoS**.

Step 2 In the **QoS – Policy** area, click **Add** to create a new QoS Policy or click the one you want to edit.

Step 3 Add **Add Class Map** and enter the details.

Step 4 Click **Save**.

Step 5 Click **Update and Apply to Device**.

Creating a Class Map (CLI)

Note Configuration of class maps via CLI offer more options and can be more granular than GUI.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_user`	Specifies the class map type and name.
Step 3	**match username** *username* **Example:** `Device(config-filter-control-classmap)# match username ciscoise`	Specifies the class map attribute filter criteria.
Step 4	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_userrole`	Specifies the class map type and name.
Step 5	**match user-role** *user-role* **Example:** `Device(config-filter-control-classmap)# match user-role engineer`	Specifies the class map attribute filter criteria.
Step 6	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_oui`	Specifies the class map type and name.

	Command or Action	Purpose
Step 7	**match oui** *oui-address* **Example:** `Device(config-filter-control-classmap)# match oui 48.f8.b3`	Specifies the class map attribute filter criteria.
Step 8	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_mac`	Specifies the class map type and name.
Step 9	**match mac-address** *mac-address* **Example:** `Device(config-filter-control-classmap)# match mac-address 0040.96b9.4a0d`	Specifies the class map attribute filter criteria.
Step 10	**class-map type control subscriber match-any** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-any cls_devtype`	Specifies the class map type and name.
Step 11	**match device-type** *device-type* **Example:** `Device(config-filter-control-classmap)# match device-type windows`	Specifies the class map attribute filter criteria.
Step 12	**class-map type control subscriber match-all** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-all match_tod`	Specifies the class map type and name.
Step 13	**match join-time-of-day** *start-time end-time* **Example:** `Device(config-filter-control-classmap)# match join-time-of-day 10:30 12:30`	Specifies a match to the time of day. Here, join time is considered for matching. For example, if the match filter is set from 11:00 am to 2:00 pm, a device joining at 10:59 am is not considered, even if it acquires credentials after 11:00 am. Here, *start-time* and *end-time* specifies the 24-hour format. Use the **show class-map type control subscriber name** *name* command to verify the configuration.

	Command or Action	Purpose
		Note You should also disable AAA override for this command to work.
Step 14	**match day** *day-of-week* **Example:** `Device(config-filter-control-classmap)# match day Monday`	Matches day of the week. Use the **show class-map type control subscriber name** *name* command to verify the configuration.
Step 15	**class-map type control subscriber match-all** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-all match_eap`	Specifies the class map type and filter as EAP.
Step 16	**match eap-type** *eap-type* **Example:** `Device(config-filter-control-classmap)# match eap-type peap`	Specifies the policy match with EAP type. Use the **show class-map type control subscriber name** *name* command to verify the configuration.
Step 17	**class-map type control subscriber match-all** *class-map-name* **Example:** `Device(config)# class-map type control subscriber match-all match_device`	Specifies the class map type and filter as device.
Step 18	**match device-type** *device-name* **Example:** `Device(config-filter-control-classmap)# match device-type android`	Matches name using the device type. Type a question mark (?) after the device type and select the device from the list. **Note** You should enable the device classifier for the device list to be populated.

Creating a Service Template (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policy**.

Step 2 On the **Local Policy** page, **Service Template** tab, click **ADD**.

Step 3 In the **Create Service Template** window, enter the following parameters:

- **Service Template Name:** Enter a name for the template.
- **VLAN ID:** Enter the VLAN ID for the template. Valid range is between 1 and 4094.

- **Session Timeout (secs):** Sets the timeout duration for the template. Valid range is between 1 and 65535.
- **Access Control List:** Choose the Access Control List from the drop-down list.
- **Ingress QOS:** Choose the input QoS policy for the client from the drop-down list
- **Egress QOS:** Choose the output QoS policy for the client from the drop-down list.

Step 4 Click **Save & Apply to Device**.

Creating a Service Template (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**service-template** *service-template-name* **Example:** `Device(config)# service-template svc1`	Enters service template configuration mode.
Step 3	**vnid** *vnid* **Example:** `Device(config-service-template)# vnid test`	Specifies the VXLAN network identifier (VNID). Use the **show service-template** *service-template-name* command to verify the configuration.
Step 4	**access-group** *access-list-name* **Example:** `Device(config-service-template)# access-group acl-auto`	Specifies the access list to be applied.
Step 5	**vlan** *vlan-id* **Example:** `Device(config-service-template)# vlan 10`	Specifies VLAN ID. Valid range is from 1-4094.
Step 6	**absolute-timer** *timer* **Example:** `Device(config-service-template)# absolute-timer 1000`	Specifies session timeout value for a service template. Valid range is from 1-65535.
Step 7	**service-policy qos input** *qos-policy* **Example:**	Configures an input QoS policy for the client.

	Command or Action	Purpose
	`Device(config-service-template)# service-policy qos input in_qos`	
Step 8	**service-policy qos output** *qos-policy* **Example:** `Device(config-service-template)# service-policy qos output out_qos`	Configures an output QoS policy for the client.

Creating a Parameter Map

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Device(config)# parameter-map type subscriber attribute-to-service param`	Specifies the parameter map type and name.
Step 3	*map-index***map device-type eq***filter-name* **Example:** `Device(config-parameter-map-filter)# 1 map device-type eq "windows" mac-address eq 3c77.e602.2f91 username eq "cisco"`	Specifies the parameter map attribute filter criteria. Multiple filters are used in the example provided here.
Step 4	*map-index***service-template***service-template-name* **precedence** *precedence-num* **Example:** `Device(config-parameter-map-filter-submode)# 1 service-template svc1 precedence 150`	Specifies the service template and its precedence.

Creating a Policy Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policy** > **Policy Map** tab..

Step 2 Enter a name for the Policy Map in the **Policy Map Name** text field.

Step 3 Click **Add**

Step 4 Choose the service template from the **Service Template** drop-down list.

Step 5 For the following parameters select the type of filter from the drop-down list and enter the required match criteria

- Device Type
- User Role
- User Name
- OUI
- MAC Address

Step 6 Click **Add Criteria**

Step 7 Click **Update & Apply to Device**.

Creating a Policy Map (CLI)

Before you begin

Before removing a policy map or parameter map, you should remove it from the target or shut down the WLAN profile or delete the session.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map type control subscriber** *policy-map-name* **Example:** `Device(config)# policy-map type control subscriber polmap5`	Specifies the policy map type.
Step 3	**event identity-update match-all** **Example:** `Device(config-event-control-policymap)# event identity-update match-all`	Specifies the match criteria to the policy map.
Step 4	You can apply a service template using either a class map or a parameter map, as shown here. • *class-num* **class** *class-map-name* **do-until-failure**	Configures the local profiling policy class map number and specifies how to perform the action or activates the service template or maps an identity-update attribute to an auto-configured template.

	Command or Action	Purpose

	• *action-index* **activate service-template** *service-template-name*
	• *action-index* **map attribute-to-service table** *parameter-map-name*
	Example:
	The following example shows how a class-map with a service-template has to be applied:
	`Device(config-class-control-policymap)# 10 class cls_mac do-until-failure`
	`Device(config-action-control-policymap)# 10 activate service-template svc1`
	Example:
	The following example shows how a parameter map has to be applied (service template is already associated with the parameter map 'param' while creating it):
	`Device(config-action-control-policymap)#1 map attribute-to-service table param`	

Step 5	**end** **Example:** `Device(config-action-control-policymap)# end`	Exits configuration mode.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 7	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)# wireless profile policy wlan-policy-profilename`	Configures a wireless policy profile. **Caution** Do not configure aaa-override for native profiling under a named wireless profile policy. Native profiling is applied at a lower priority than AAA policy. If aaa-override is enabled, the AAA policies will override native profile policy.
Step 8	**description** *profile-policy-description* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile.
Step 9	**dhcp-tlv-caching** **Example:**	Configures DHCP TLV caching on a WLAN.

	Command or Action	Purpose
	`Device(config-wireless-policy)# dhcp-tlv-caching`	
Step 10	**http-tlv-caching** **Example:** `Device(config-wireless-policy)# http-tlv-caching`	Configures client HTTP TLV caching on a WLAN.
Step 11	**subscriber-policy-name** *policy-name* **Example:** `Device(config-wireless-policy)# subscriber-policy-name polmap5`	Configures the subscriber policy name.
Step 12	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 1`	Configures a VLAN name or VLAN ID.
Step 13	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Saves the configuration.

Configuring Native Profiling in Local Mode

To configure native profiling in the local mode, you must follow the steps described in #unique_1935. In the policy profile, you must enable central switching as described in the step given below in order to configure native profiling.

Procedure

	Command or Action	Purpose
Step 1	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Enables central switching.

Verifying Native Profile Configuration

Use the following **show** commands to verify the native profile configuartion:

```
Device# show wireless client device summary

Active classified device summary
MAC Address       Device-type                       User-role
Protocol-map
-----------------------------------------------------------------------------------------------
```

```
1491.82b8.f94b    Microsoft-Workstation             sales
           9
1491.82bc.2fd5    Windows7-Workstation              sales
          41


Device# show wireless client device cache

Cached classified device info

MAC Address       Device-type                       User-role
Protocol-map
------------------------------------------------------------------------------------------------
2477.031b.aa18    Microsoft-Workstation
           9
30a8.db3b.a753    Un-Classified Device
           9
4400.1011.e8b5    Un-Classified Device
           9
980c.a569.7dd0    Un-Classified Device
```

```
Device# show wireless client mac-address 4c34.8845.e32c detail | s
Session Manager:
  Interface :
  IIF ID            : 0x90000002
  Device Type       : Microsoft-Workstation
  Protocol Map      : 0x000009
  Authorized        : TRUE
  Session timeout   : 1800
  Common Session ID: 783802090000000174BF2B5B9
  Acct Session ID   : 0
  Auth Method Status List
   Method : MAB
    SM State         : TERMINATE
    Authen Status    : Success
  Local Polices:
   Service Template : wlan_svc_C414.3CCA.0A51 (priority 254)
    Absolute-Timer   : 1800
  Server Polices:
  Resultant Policies:
  Filter-ID         : acl-auto
  Input QOS         : in_qos
  Output QOS        : out_qos
  Idle timeout      : 60 sec
  VLAN               : 10
  Absolute-Timer    : 1000
```

Use the following **show** command to verify the class map details for a class map name:

```
Device# show class-map type control subscriber name test
Class-map               Action                       Exec  Hit  Miss  Comp
---------                ------                       ----  ---  ----   ---
match-any test     match day Monday                    0     0    0     0
match-any test     match join-time-of-day 8:00 18:00   0     0    0     0
Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
       condition without a need to continue on to the end
```

CHAPTER 142

Air Time Fairness

- Information About Air Time Fairness, on page 1561
- Restrictions on Cisco Air Time Fairness, on page 1563
- Cisco Air Time Fairness (ATF) Use Cases, on page 1564
- Configuring Cisco Air Time Fairness (ATF), on page 1564
- Verifying Cisco ATF Configurations, on page 1568
- Verifying Cisco ATF Statistics, on page 1568

Information About Air Time Fairness

Cisco Air Time Fairness (ATF) allows network administrators to group devices of a defined category and enables some groups to receive traffic from the WLAN more frequently than the other groups. Therefore, some groups are entitled to more air time than the other groups.

Cisco ATF has the following capabilities:

- Allocates Wi-Fi air time for user groups or device categories.
- Air time fairness is defined by the network administrator and not by the network.
- Provides a simplified mechanism for allocating air time.
- Dynamically adapts to changing conditions in a WLAN.
- Enables a more efficient fulfillment of service-level agreements.
- Augments standards-based Wi-Fi QoS mechanisms.

By enabling network administrators to define what fairness means in their environments with regards to the amount of air time per client group, the amount of traffic is also controlled.

To control air time on a percentage basis, the air time including both uplink and downlink transmissions of a client or SSID is continuously measured.

Only air time in the downlink direction, that is AP to client, can be controlled accurately by the AP. Although air time in the uplink direction, that is client to AP can be measured, it cannot be controlled. Although the AP can constrain air time for packets that it sends to clients, the AP can only measure air time for packets that it hears from clients because it cannot strictly limit their air time.

Cisco ATF establishes air time limits (defined as a percentage of total air time) and applies those limits on a per SSID basis, where the SSID is used as a parameter to define a client group. Other parameters can be used as well to define groups of clients. Furthermore, a single air time limit can be applied to individual clients.

If the air time limit for an SSID (or client) is exceeded, the packets in the downlink direction are dropped. Dropping downlink packets (AP to client) frees up air time whereas dropping uplink packets (client to AP) does not do anything to free up air time because the packet has already been transmitted over the air by the client.

Client Fair Sharing

Cisco Air Time Fairness can be enforced on clients that are associated with an SSID or WLAN. This ensures that all clients in an SSID or WLAN are treated equally based on their utilization of the radio bandwidth. This feature is useful in scenarios where one or a few clients could use the complete air time allocated for an SSID or WLAN, thereby depriving Wi-Fi experience for other clients associated with the same SSID or WLAN.

- The percentage of air time to be given to each client is recomputed every time a client connects or disconnects.
- Client fair sharing is applicable only to downstream traffic.
- Clients can be categorized into usage groups at the policy level.
- Client-based ATF metrics accumulation is performed in the transmit complete routine. This allows the air time that is unused by clients in low-usage or medium-usage groups to be accumulated to a common share pool bucket where the high-usage clients can be replenished.

Supported Access Point Platforms

Cisco ATF is supported on the following APs:

- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points

Note Cisco ATF is supported on MESH, if APs support ATF. ATF is supported on FlexConnect mode and the Local mode.

Note Cisco Catalyst APs offer capabilities that are equivalent to ATF by leveraging the enhancements in the Wi-Fi 6 and 6E protocols. 802.11ax features such as OFDMA, bidirectional MU-MIMO, and BSS coloring, combined with the advanced QoS features in the Cisco Catalyst 9800 Series Wireless Controllers, help resolve scheduling and congestion problems, accommodate multiple users at the same time, and allocate bandwidth more efficiently.

Cisco ATF Modes

Cisco ATF operates in the following modes:

- Monitor mode in which users can do the following:
  - View the air time
  - Report air time usage for all AP transmissions
  - View reports
    - per SSID or WLAN
    - per site group/tag
  - Report air time usage at periodic intervals
  - No enforcement as part of Monitor mode
- Enforce Policy mode in which users can do the following:
  - Enforce air time based on configured policy
  - Enforce air time on the following:
    - A WLAN
    - All APs connected in a Cisco Catalyst 9800 Series Wireless Controller network
    - per site group/tag

Restrictions on Cisco Air Time Fairness

- Cisco ATF can be implemented only on data frames in the downstream direction.
- When ATF is configured in per-SSID mode, all the WLANs are disabled before you enter any ATF configuration commands. The WLANs are enabled after you enter all the ATF commands.

Cisco Air Time Fairness (ATF) Use Cases

Public Hotspots (Stadium/Airport/Convention Center/Other)

In this instance, a public network is sharing a WLAN between two (or more) service providers and the venue. Subscribers to each service provider can be grouped and allocated a certain percentage of air time.

Education

In this instance, a university is sharing a WLAN between students, faculty, and guests. The guest network can be further partitioned by the service provider, for distribution of bandwidth privileges to the guests. Each group can be assigned a certain percentage of air time.

Enterprise/Hospitality/Retail

In this instance, the venue is sharing a WLAN between employees and guests. The guest network can be further partitioned by service provider. The guests could be sub-grouped by tier of service type with each subgroup being assigned a certain percentage of air time, for example a paid group is entitled for more air time than the free group.

Time Shared Managed Hotspot

In this instance, the business entity managing the hotspot, such as a service provider or an enterprise, can allocate and subsequently lease air time to other business entities.

Configuring Cisco Air Time Fairness (ATF)

Configuring Cisco Air Time Fairness

The following are the high-level steps to configure Cisco ATF:

1. Enable Monitor mode to determine network usage (optional).
2. Create Cisco ATF policies.
3. Add WLAN ATF policies per network or per site group/tag.
4. Determine, if optimization must be enabled.
5. Periodically check the Cisco ATF statistics.

Creating a Cisco ATF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Air Time Fairness**.

Step 2 Click the **Profiles** tab and click the **Add** button, to create a new ATF policy.
The **Add ATF Policy** window is displayed.

Step 3 Specify a name, ID, and weight to the ATF policy. Weighted ratio is used instead of percentages so that the total can exceed 100. The minimum weight that you can set is 5. For example, if you configure the weight as 50, this means that the air time for this ATF profile is 50% when applied to an policy profile.

Step 4 Use the slider to enable or disable the **Client Sharing** feature. When you enable this option in the Web UI, the default ATF configuration is set to **Enforce** and not **Monitor**.

Step 5 Click **Apply to Device**.

Creating Cisco ATF Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile airtime-fairness** *atf-policy-name atf-profile-id* **Example:** `Device(config)# wireless profile airtime-fairness atf-policy-name 1`	Creates a new Cisco ATF policy. • *atf-policy-name*—Enters the ATF profile name. • *atf-profile-id*—Enters the ATF profile ID. Range is from 0 to 511.
Step 3	**weight** *policy-weight* **Example:** `Device(config-config-atf)# weight 5`	Adds a weight to the Cisco ATF policy. • *policy-weight*—Enters the policy weight. Range is from 5 to 100.
Step 4	**client-sharing** **Example:** `Device(config-config-atf)# client-sharing`	Enables or disables the client sharing for Cisco ATF policy.
Step 5	**end** **Example:** `Device(config-config-atf)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching Cisco ATF Profile to a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**. **Policy**.

Step 2 Click **Add**.
The **Add Policy Profile** window is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Under the **Air Time Fairness Policies** section, select the required policy for 2.4 GHz and 5 GHz policies.

Step 5 Click **Apply to Device**.

Attaching Cisco ATF Profile to a Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy profile-name`	Creates policy profile for the WLAN. • *profile-name* —Is the profile name of the policy profile.
Step 3	**dot11** {**24ghz** | **5ghz**} **airtime-fairness** *atf-policy-name* **Example:** `Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy-name`	Configures air time fairness policy for 2.4- or 5-GHz radio. • *atf-policy-name*—Is the name of the air time fairness policy. For more details on creating Cisco ATF policy, refer to the Creating Cisco ATF Policy. **Note** You can assign the same ATF policy to both 2.4-GHz and 5-GHz radios (or) have two different ATF policies as well.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling ATF in the RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 Click **Add**.
The **Add RF Profile** window is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Under the **ATF Configuration** section, complete the following :

a) Use the slider to enable or disable the **Status**. The **Mode** field is displayed.

b) Click the **Monitor** mode or **Enforced** mode radio option. If you enable the **Enforced** mode, use the slider to enable or disable **Optimization**.

c) Use the slider to enable to disable **Bridge Client Access**. This is applicable for mesh mode APs. Bridge Client Access determines the percentage of the ATF policy weight that is allocated to clients connected to the mesh APs.

Step 5 Specify the **Airtime Allocation** value between 5 and 90.

Step 6 Click **Apply to Device**.

Enabling ATF in the RF Profile (CLI)

Cisco ATF must be enabled on 2.4 GHz or 5 GHz radios separately.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile for 2.4- or 5-GHz radio.
Step 3	**airtime-fairness mode** {**enforce-policy** | **monitor**} **Example:** `Device(config-rf-profile)# airtime-fairness mode enforce-policy`	Configures air time fairness in either of the modes: • Enforce-policy—This mode signifies that the ATF is operational. • Monitor—This mode gathers information about air time and reports air time usage.
Step 4	**airtime-fairness optimization**	Enables the air time fairness optimization.

	Command or Action	Purpose
	Example: `Device(config-rf-profile)# airtime-fairness optimization`	Optimization is effective when the current WLAN reaches the air time limit and the other available WLANs does not use air time to its full extent.
Step 5	**end** **Example:** `Device(config-rf-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Cisco ATF Configurations

You can verify Cisco ATF configurations using the following commands:

Table 116: Commands for Verifying Cisco ATF Configurations

Commands	Description
show wireless profile airtime-fairness summary	Displays the summary of air time fairness profiles.
show wireless profile airtime-fairness mapping	Displays the ATF policy mapping with the wireless profiles.
show ap airtime-fairness summary	Displays the ATF configuration summary of all radios.
show ap dot11 24ghz airtime-fairness	Displays the ATF configuration for 2.4-GHz radio.
show ap dot11 5ghz airtime-fairness	Displays the ATF configuration for 5-GHz radio.
show ap name *ap-name* **airtime-fairness**	Displays the ATF configuration or statistics for an AP.
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness statistics summary**	Displays the ATF statistics of 2.4- or 5GHz radio.

Verifying Cisco ATF Statistics

Table 117: ATF Statistics per WLAN

Commands	Description
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness wlan** *wlan_name* **statistics**	Displays the ATF statistics related to a WLAN.

Table 118: ATF Statistics per ATF Policy

Commands	Description
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness policy** *policy-name* **statistics**	Displays the ATF statistics related to an ATF policy.

Table 119: ATF Statistics per Client

Commands	Description
show ap airtime-fairness statistics client *mac_address*	Displays the ATF statistics related to a client.

CHAPTER 143

IPv6 Non-AVC QoS Support

- Information About IPv6 Non-AVC QoS Support, on page 1571
- Configuring IPv6 Non-AVC QoS, on page 1571
- Verifying IPv6 Non-AVC QoS, on page 1574

Information About IPv6 Non-AVC QoS Support

From Cisco IOS XE Amsterdam 17.2.1, the IPv6 Non-AVC QoS feature is supported on Fabric and FlexConnect local switching, where QoS is performed at the AP, on par with the IPv4 functionality.

Note This feature is not supported on Cisco Aironet 1700 Series Access Points, Cisco Aironet 2700 Series Access Points, and Cisco Aironet 3700 Series Access Points.

The following actions are supported for IPv6 Non-AVC QoS:

- Marking the DSCP value for IPv6 packets
- Dropping IPv6 packets based on the DSCP value
- Policing IPv6 traffic

Configuring IPv6 Non-AVC QoS

The following sections contain information about the various configurations that comprise the configuration of IPv6 Non-AVC QoS:

Marking DSCP Values for an IPv6 Packet

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map testpolicy`	Creates a policy map.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)#class testmap`	Creates a policy criteria.
Step 4	**set dscp** *<0-63>* **Example:** `Device(config-pmap-c)#set dscp 34`	Sets the DSCP value in an IPv6 packet between 0 and 63.

Dropping an IPv6 Packet with DSCP Values

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map drop_dscp`	Creates a policy map.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)#class drop_dscp_class`	Creates a policy criteria.
Step 4	**police cir** *<8000 - 10000000000>* **Example:** `Device(config-pmap-c)#police cir 8000`	Polices the committed information rate between 8000 and 10000000000. Target bit rate (Bits per second).

	Command or Action	Purpose
Step 5	**conform-action drop** **Example:** `Device(config-pmap-c-police)#conform action drop`	Configures the **conform-action drop** command, the action when the rate is less than the conform burst.
Step 6	**exceed-action drop** **Example:** `Device(config-pmap-c-police)#exceed-action drop`	Configures the **exceed-action drop** command, the action when the rate is within the conform and conform plus exceed burst.

Policing IPv6 Traffic

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map drop_dscp`	Creates a policy map.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)#class drop_dscp_class`	Creates a policy criteria.
Step 4	**police cir** *<8000 - 10000000000>* **Example:** `Device(config-pmap-c)#police cir 8000`	Polices the committed information rate between 8000 and 10000000000. Target bit rate (Bits per second).
Step 5	**conform-action transmit** **Example:** `Device(config-pmap-c-police)#conform-action transmit`	Configures the **conform-action transmit** command, for transmitting packets.
Step 6	**exceed-action drop** **Example:** `Device(config-pmap-c-police)#exceed-action drop`	Configures the **exceed-action drop** command, the action when the rate is within conform and conform plus exceed burst.

Verifying IPv6 Non-AVC QoS

- To verify the DSCP values for IPv6 packets, IPv6 packets that are dropped, and the policing of IPv6 traffic, use the **show policy-map** command:

  The following is a sample output of the **show** command that verifies the DSCP value for an IPv6 packet:

```
Device# show policy-map
1 policymaps
Policy Map Set-dscp type:qos client:default
 Class Set-dscp1_ADV_UI_CLASS
 set dscp af41 (34)
 Class class-default
 no actions
```

- The following is a sample output of the **show** command that verifies the IPv6 packets that are dropped:

```
Device# show policy-map
1 policymaps
Policy Map Drop-dscp type:qos client:default
        Class Drop-dscp1_ADV_UI_CLASS
        drop

        Class class-default
        no actions
```

- The following is a sample output of the **show** command that verifies the policing of IPv6 traffic:

```
Device# show policy-map
1 policymaps
Policy Map Drop-traffic type:qos client:default
        Class Drop-traffic1_ADV_UI_CLASS
        police rate 2000000 bps (250000Bytes/s)
        conform-action
        exceed-action

        Class class-default
        no actions
```

CHAPTER 144

QoS Basic Service Set Load

- Information About QoS Basic Set Service Load, on page 1575
- Configuring QBSS Load, on page 1576
- Verifying QoS Basic Set Service Load, on page 1577

Information About QoS Basic Set Service Load

The QoS Basic Set Service (QBSS) information element (IE) knob is a per-WLAN configuration that is configured to include or exclude the QBSS IE, which is sent in beacon frames and probe responses. QBSS IE advertises the channel load information of an AP. The QBSS IE functionality is enabled by default.

Until Cisco IOS XE Amsterdam 17.1.1s, the enablement of Wi-Fi Multimedia (WMM) automatically enabled the QBSS load advertisement in the probes and beacons and there was no separate knob to turn on QBSS load IE. However, from Cisco IOS XE Amsterdam 17.2.1, this behavior has changed with the introduction of a separate configuration knob.

Until Cisco IOS XE Amsterdam 17.1.1s:

- When WMM was enabled on WLAN, QBSS load was advertised in the beacon and probe frames.
- When WMM was disabled on WLAN, QBSS IE was not advertised in the beacon and probe frames.

From Cisco IOS XE Amsterdam 17.2.1,

- When you enable WMM and QBSS ID on WLAN, QBSS IE is advertised in the beacon and probe frames.
- When you enable WMM on WLAN and disable QBSS load IE on WLAN, QBSS load is not advertised in the beacon and probe frames.
- When you disable WMM on WLAN and enable QBSS load IE on WLAN, QBSS IE is advertised in the beacon and probe frames.

Note By default, QBSS load IE is enabled. The behavior can be configured on policy profile.

Configuring QBSS Load

The following sections contain information about the various configurations that comprise the configuration of QoS basic service set load.

Configuring Wi-Fi Multimedia

Perform the procedure given below to create a WLAN and then enable WMM.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*] **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID: • *profile-name*: Profile name of the WLAN. You can use between 1 to 32 alphanumeric characters. • *wlan-id*: WLAN ID. You can use between 1 to 512 alphanumeric characters. • *ssid*: Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** By default, the WLAN is disabled.
Step 3	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for Advanced Encryption Standard (AES).
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**wmm** {**allowed** | **require**} **Example:** `Device(config-wlan)#wmm allowed`	Configures WMM and allows WMM on the WLAN.
Step 6	**no shutdown** **Example:**	Enables WLAN.

	Command or Action	Purpose
	`Device(config-wlan)#no shutdown`	

Enabling QoS Basic Set Service Load

Perform the procedure given below to enable QBSS load.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 24`	Configures VLAN name or VLAN ID.
Step 4	**[no] qbss-load** **Example:** `Device(config-wireless-policy)#[no] qbss-load`	Enables QoS enhanced basic service set information element. (Use the **no** form of this command to disable the feature.)
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

What to do next

1. Create a policy tag. For more information about creating policy tags, refer to *Configuring a Policy Tag (CLI)*.
2. Map the policy tag to the AP. For more information about mapping a policy tag to the AP, refer to *Attaching a Policy Tag and Site Tag to an AP (CLI)*.

Verifying QoS Basic Set Service Load

To verify if QBSS load is enabled, use the **show wireless profile policy detailed** *named-policy-profile* command:

```
Device# show wireless profile policy detailed named-policy-profile
```**show wireless profile policy detailed** *named-policy-profile*

```
Policy Profile Name                : named-policy-profile
Description                        :
Status                             : ENABLED
VLAN                               : 91
Multicast VLAN                     : 0
OSEN client VLAN                   :
Multicast Filter                   : DISABLED
QBSS Load                          : ENABLED
Passive Client                     : DISABLED
ET-Analytics                       : DISABLED
StaticIP Mobility                  : DISABLED
WLAN Switching Policy
  Flex Central Switching           : ENABLED
  Flex Central Authentication      : ENABLED
  Flex Central DHCP                : ENABLED
  Flex NAT PAT                     : DISABLED
  Flex Central Assoc               : ENABLED
```

PART XI

IPv6

- IPv6 Client IP Address Learning, on page 1581
- IPv6 ACL, on page 1601
- IPv6 Client Mobility, on page 1613
- IPv6 Support on Flex and Mesh, on page 1617
- IPv6 CAPWAP UDP Lite Support, on page 1621
- Neighbor Discovery Proxy, on page 1623
- Address Resolution Protocol Proxy, on page 1627
- IPv6 Ready Certification, on page 1629

CHAPTER 145

IPv6 Client IP Address Learning

- Information About IPv6 Client Address Learning, on page 1581
- Prerequisites for IPv6 Client Address Learning, on page 1585
- IPv6 Address Tracking for Wireless Clients, on page 1585
- Configuring RA Throttle Policy (CLI), on page 1586
- Applying RA Throttle Policy on VLAN (GUI), on page 1587
- Applying RA Throttle Policy on a VLAN (CLI), on page 1588
- Configuring IPv6 Interface on a Switch (GUI), on page 1588
- Configuring IPv6 on Interface (CLI), on page 1589
- Configuring DHCP Pool on Switch (GUI), on page 1590
- Configuring DHCP Pool on Switch (CLI), on page 1590
- Configuring Stateless Auto Address Configuration Without DHCP on Switch (CLI), on page 1591
- Configuring Stateless Auto Address Configuration With DHCP on Switch , on page 1593
- Configuring Stateless Address Auto Configuration Without DHCP on Switch (CLI), on page 1594
- Native IPv6, on page 1595

Information About IPv6 Client Address Learning

Client Address Learning is configured on device to learn the IPv4 and IPv6 address of wireless client, and the client's transition state maintained by the device on association and timeout.

There are three ways for an IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLAAC)
- Stateful DHCPv6
- Static Configuration

In all of these methods, the IPv6 client always sends a neighbor solicitation Duplicate Address Detection (DAD) request to ensure that there is no duplicate IP address on the network. The device snoops on the Neighbor Discovery Protocol (NDP) and DHCPv6 packets of the client to learn about its client IP addresses.

Address Assignment Using SLAAC

The most common method for IPv6 client address assignment is SLAAC, which provides simple plug-and-play connectivity, where clients self-assign an address based on the IPv6 prefix.

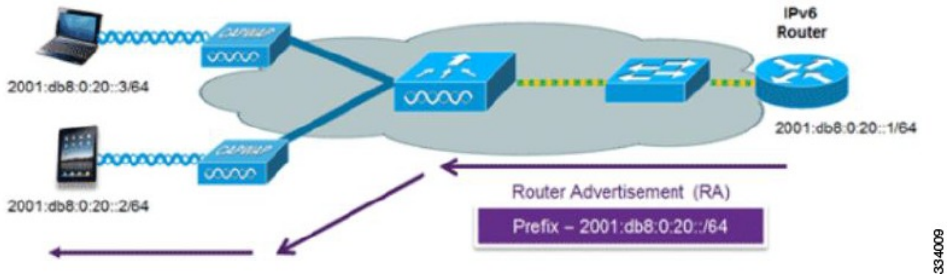
SLAAC is configured as follows:

- A host sends a Router Solicitation message.
- The host waits for a Router Advertisement message.
- The host take the first 64 bits of the IPv6 prefix from the Router Advertisement message and combines it with the 64 bit EUI-64 address (in the case of Ethernet, this is created from the MAC address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the Router Advertisement message, as its default gateway.
- Duplicate Address Detection is performed by the IPv6 clients to ensure that random addresses that are picked do not collide with other clients.

Note The last 64 bits of the IPv6 address can be learned by using one of the following algorithms:

- EUI-64, which is based on the MAC address of the interface
- Private addresses that are randomly generated

Figure 47: Address Assignment Using SLAAC



The following Cisco IOS configuration commands from a Cisco-capable IPv6 router are used to enable SLAAC addressing and router advertisements:

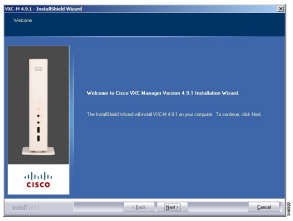
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

Stateful DHCPv6 Address Assignment

The use of DHCPv6 is not required for IPv6 client connectivity if SLAAC is already deployed. There are two modes of operation for DHCPv6, that is, Stateless and Stateful.

The DHCPv6 Stateless mode is used to provide clients with additional network information that is not available in the router advertisement, but not an IPv6 address, becuase this is already provided by SLAAC. This information includes the DNS domain name, DNS servers, and other DHCP vendor-specific options.

Figure 48: Stateful DHCPv6 Address Assignment



The following interface configuration is for a Cisco IOS IPv6 router implementing stateless DHCPv6 with SLAAC enabled:

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

Router Solicitation

A Router Solicitation message is issued by a host controller to facilitate local routers to transmit a Router Advertisement from which the controller can obtain information about local routing, or perform stateless auto configuration. Router Advertisements are transmitted periodically and the host prompts with an immediate Router Advertisement using a Router Solicitation such as - when it boots or following a restart operation.

Router Advertisement

A Router Advertisement message is issued periodically by a router or in response to a Router Solicitation message from a host. The information contained in these messages is used by a host to perform stateless auto configuration and to modify its routing table.

Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery, and ICMP Redirect used in IPv4.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 Neighbor Discovery packets that do not comply, are dropped. The neighbor binding table in the tracks each IPv6 address and its associated MAC address. Clients are removed from the table according to neighbor-binding timers.

Neighbor Discovery Suppression

The IPv6 addresses of wireless clients are cached by a device once the wireless client is in RUN state. When the device receives an NS multicast, it looks into the IPv6 addresses cached. If the target address is known to the device and belongs to one of its wireless clients, the device converts the NS from multicast to unicast and forward it to the wireless client. If the target address is not present in the cache, then device interprets that the Multicast NS is for a wired entity and forward it towards the wired side and not to the wireless client.

The same behavior is seen for ARP request in case of IPv4 address, where the device maintains IPv4 address of the wireless client in the cache.

When neither of the configuration is enabled, and when the device receives Non-DAD or DAD NS multicast looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will convert the multicast NS to unicast NS, with the destination MAC address, replaced with client's MAC and forward the unicast packet towards client.

When full-proxy is enabled, and when the device receives Non-DAD or DAD NS multicast, looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will reply with an NA message on behalf of the client.

You can use the **ipv6 nd proxy** command to enable or disable DAD or full proxy.

When the device receives an DAD-NS multicast looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will reply with an NA message on behalf of the client.

When the device receives Non-DAD NS multicast looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will convert the multicast NS to unicast NS, with the destination MAC address, replaced with client's MAC and forward the unicast packet towards client.

If the device does not have the IPv6 address of a wireless client, the device does not respond with NA; instead, it forwards the NS packet to the wired side. Reason for forwarding to Wired Side is due to the assumption that all wireless client IPv6 address and the its mapped MAC address should be available in the controller and if an IPv6 address required in the NS is not available, then that address is not a wireless client address, so forwarded to wired side.

Router Advertisement Guard

The RA Guard feature increases the security of the IPv6 network by dropping router advertisements coming from wireless clients. Without this feature, misconfigured or malicious IPv6 clients could announce themselves as a router for the network, often with a high priority, which could take precedence over legitimate IPv6 routers. By default, RA guard is always enabled on the controller.

- Port on which the frame is received
- IPv6 source address
- Prefix list
- Trusted or Untrusted ports for receiving the router advertisement guard messages
- Trusted/Untrusted IPv6 source addresses of the router advertisement sender
- Trusted/Untrusted Prefix list and Prefix ranges
- Router preference

Router Advertisement Throttling

RA throttling allows the controller to enforce limits to the RA packets headed toward the wireless network. By enabling RA throttling, routers that send multiple RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicast to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

Prerequisites for IPv6 Client Address Learning

Before configuring IPv6 client address learning, configure the clients to support IPv6.

To enable wireless IPv6 client connectivity, the underlying wired network must support IPv6 routing and an address assignment mechanism, such as SLAAC or DHCPv6. The wireless LAN controller must have L2 adjacency to the IPv6 router.

Note The AP learns IPv6 client address based on source IP address even though Neighbor Advertisements can hold rest of the IPv6 addresses. AP won't look into the Neighbor Advertisements to learn the IPv6 address learnt by the client. This behavior is seen only on Apple clients and not on Microsoft Windows clients.

IPv6 Address Tracking for Wireless Clients

Until Cisco IOS XE 17.9.1, the controller supported a maximum of eight IPv6 addresses per wireless client. After eight IPv6 addresses were learnt for a wireless client, the controller dropped that wireless client's data traffic coming with new IPv6 source addresses.

However, in Cisco IOS XE 17.9.2 release, the controller allows data traffic of the wireless clients coming with new IPv6 source addresses even after eight addresses have been learnt for respective wireless clients. The controller continues to learn new iPv6 addresses of the wireless clients from the wireless clients' control traffic (IPv6 NS/NA and DHCPv6), and keeps track of only a maximum of eight addresses per wireless client.

To allow forwarding of the multicast neighbor solicitation (NS) queries for unknown IPv6 target addresses of wireless clients (the client addresses that are not tracked by the controller) to wireless clients, the **wireless ipv6 nd ns-forward** configuration must be enabled.

Important We recommend that you configure IPv6 Multicast over Multicast (MoM) tunnel along with the **wireless ipv6 nd ns-forward** configuration.

Note In Cisco IOS XE 17.9.2, since the controller allows IPv6 traffic without address tracking beyond the eight IPv6 address limit, some of the features such as, User Defined Network, iPSK Peer-to-Peer Blocking, Management over Wireless, Neighbor Discovery Suppression, IP Theft Detection, and so on, may not work for the wireless clients using more than eight addresses. You can disable the new behavior by enabling the IP Source Guard feature https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg/m_ipsg_ewlc.html?bookSearch=true.

Configuring Unknown Address Multicast Neighbor Solicitation Forwarding

To allow forwarding of the multicast neighbor solicitation (NS) queries for unknown IPv6 target addresses of wireless clients (the client addresses that are not tracked by the controller) to wireless clients, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless ipv6 nd ns-forward** **Example:** `Device (config)# wireless ipv6 nd ns-forward`	Enables forwarding of the multicast neighbor solicitation (NS) messages for unknown IPv6 target addresses of wireless clients (the client addresses that are not tracked by the controller) to wireless clients. **Note** **We recommend that you configure IPv6 Multicast over Multicast (MoM) tunnel along with this configuration.**

Configuring RA Throttle Policy (CLI)

Configure RA Throttle policy to allow the enforce the limits

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ipv6 nd ra-throttler policy ra-throttler1** **Example:** `Device(config)# ipv6 nd ra-throttler policy ra-throttler1`	Define the router advertisement (RA) throttler policy name and enter IPv6 RA throttle policy configuration mode.
Step 3	**throttleperiod 500** **Example:** `Device(config-nd-ra-throttle)# throttle-period 500`	Configures the throttle period in an IPv6 RA throttler policy. Throttle period is in seconds and it is the time while the controller will not forward RA to the wireless clients.
Step 4	**max-through 10** **Example:** `Device(config-nd-ra-throttle)# max-through 15`	Limits multicast RAs per VLAN per throttle period.
Step 5	**allow-atleast 5 at-most 10** **Example:** `Device(config-nd-ra-throttle)# allow at-least 5 at-most 10`	Limits the number of multicast RAs per device per throttle period in an RA throttler policy.

Applying RA Throttle Policy on VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **RA Throttle Policy**.

Step 2 Click **Add**. The **Add RA Throttle Policy** dialog box appears.

Step 3 Enter a name for the policy in the **Name** field.

Step 4 Choose the desired option from the **Medium Type** drop-down list.

Step 5 Enter a value in the **Throttle Period** field. RA throttling takes place only after the Max Through limit is reached for the VLAN or the Allow At-Most value is reached for a particular router.

Step 6 Enter a value for the **Max Through** field, which is the maximum number of RA packets on a VLAN that can be sent before throttling takes place. The **No Limit** option allows an unlimited number of RA packets through with no throttling.

Step 7 Choose an **Interval Option**, which allows the device to act differently based on the RFC 3775 value set in IPv6 RA packets, from the following options:

- Ignore—Causes the RA throttle to treat packets with the interval option as a regular RA and subject to throttling if in effect.
- Passthrough—Allows any RA messages with the RFC 3775 interval option to go through without throttling.

- Throttle—Causes the RA packets with the interval option to always be subject to rate limiting.

Step 8 Enter the minimum number of RA packets per router that can be sent as multicast before throttling takes place in the **At Least Multicast RAs** field.

Step 9 Enter the maximum number of RA packets per router that can be sent as multicast before throttling takes place in the **At Most Multicast RAs** field. The **No Limit** option allows an unlimited number of RA packets through the router.

Step 10 Click the **Add & Apply to Device** button.

Applying RA Throttle Policy on a VLAN (CLI)

Applying the RA Throttle policy on a VLAN. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan configuration 1** **Example:** `Device(config)# vlan configuration 1`	Configures a VLAN or a collection of VLANs and enters VLAN configuration mode.
Step 3	**ipv6 nd ra throttler attach-policy ra-throttler1** **Example:** `Device(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1`	Attaches an IPv6 RA throttler policy to a VLAN or a collection of VLANs.

Configuring IPv6 Interface on a Switch (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** > **SVI**.

Step 2 Click **Add**.

Step 3 Enter **VLAN Number**, **Description** and **MTU (Bytes)**.

Step 4 Enable or disable the **Admin Status** toggle button.

Step 5 In **IP Options**, check the **IPv6** check box.

Step 6 Choose the type of **Static** address from the drop-down list and enter the Static Address.

Step 7 Check or uncheck the **DHCP**, **Autoconfig** and **Act as an IPv6 DHCP client** check boxes.

If you check the **DHCP** check box, the **Rapid Commit** check box is displayed. Check or uncheck the **Rapid Commit** check box.

Step 8 Click **Apply to Device**.

Configuring IPv6 on Interface (CLI)

Follow the procedure given below to configure IPv6 on an interface:

Before you begin

Enable IPv6 on the client and IPv6 support on the wired infrastructure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 10`	Creates an interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the GigabitEthernet interface using the link-local option.

Step 5	**ipv6 enable** **Example:**	(Optional) Enables IPv6 on the GigabitEthernet interface.

	Command or Action	Purpose
	`Device(config)# ipv6 enable`	
Step 6	**end** **Example:** `Device(config)# end`	Exits interface mode.

Configuring DHCP Pool on Switch (GUI)

Procedure

Step 1 Choose **Administration** > **DHCP**.
Step 2 Click the **Add** button. The **Create DHCP Pool** dialog box appears.
Step 3 Enter a pool name in the **DHCP Pool Name** field. The name must not be greater than 236 characters in length.
Step 4 Choose either **IPv4** or **IPv6** from the **IP Type** drop-down list.
Step 5 Enter an IP address in the **Network** field.
Step 6 Choose any one of the available subnet masks from the **Subnet Mask** drop-down list.
Step 7 Enter an IP address in the **Starting ip** field.
Step 8 Enter an IP address in the **Ending ip** field.
Step 9 Optional, set the status of the **Reserved Only** field to **Enabled** if you wish to reserve the DHCP pool.
Step 10 Choose the desired option from the **Lease** drop-down list.
Step 11 Selecting the **User Defined** option from the **Lease** drop-down list enables the **(0-365 days)**, **(0-23 hours)**, and **(0-59 minutes)** fields. Enter appropriate values.
Step 12 Click the **Save & Apply to Device** button.
Step 13 For IPv6, Enter the **DNS Server, DNS Domain Name, and Ipv6 Address Allocation**.

Configuring DHCP Pool on Switch (CLI)

Follow the procedure given below to configure DHCP Pool on an interface:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *vlan-id* **Example:** `Device(config)# ipv6 dhcp pool 21`	Enters the configuration mode and configures the IPv6 DHCP pool on the Vlan.
Step 4	**address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10** **Example:** `Device(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10`	Enters the configuration-dhcp mode and configures the address pool and its lifetime on a Vlan.
Step 5	**dns-server 2001:100:0:1::1** **Example:** `Device(config-dhcpv6)# dns-server 2001:20:21::1`	Configures the DNS servers for the DHCP pool.
Step 6	**domain-name example.com** **Example:** `Device(config-dhcpv6)# domain-name example.com`	Configures the domain name to complete unqualified host names.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Stateless Auto Address Configuration Without DHCP on Switch (CLI)

Follow the procedure given below to configure stateless auto address configuration without DHCP:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:** `Device(config)# interface vlan 1`	Creates an interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the GigabitEthernet interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Device(config)# ipv6 enable`	(Optional) Enables IPv6 on the GigabitEthernet interface.

Step 6	**no ipv6 nd managed-config-flag**
	Example:
	`Device(config)# interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

Step 7	**no ipv6 nd other-config-flag** **Example:** `Device(config-if)# no ipv6 nd other-config-flag`	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Stateless Auto Address Configuration With DHCP on Switch

Follow the procedure given below to configure stateless auto address configuration with DHCP:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:** `Device(config)# interface vlan 1`	Creates an interface and enters interface configuration mode.

Step 4	**ip address fe80::1 link-local**
	Example:
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the GigabitEthernet interface using the link-local option.

Step 5	**ipv6 enable** **Example:** `Device(config)# ipv6 enable`	(Optional) Enables IPv6 on the GigabitEthernet interface.
Step 6	ipv6 nd prefix ipaddress **Example:** `ipv6 nd prefix 2001:9:3:54::/64 no-advertise`	Specifies a subnet prefix.
Step 7	**no ipv6 nd managed-config-flag** **Example:**	Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

	Command or Action	Purpose
	`Device(config)# interface vlan 1` `Device(config-if)# no ipv6 nd managed-config-flag`	
Step 8	**ipv6 nd other-config-flag** **Example:** `Device(config-if)# no ipv6 nd other-config-flag`	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 9	ipv6 dhcp server servername **Example:** `ipv6 dhcp server VLAN54`	Displays the configuration parameters.
Step 10	**end** **Example:** `Device(config)# end`	Exits interface mode.

Configuring Stateless Address Auto Configuration Without DHCP on Switch (CLI)

Follow the procedure given below to configure stateless auto address configuration without DHCP:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan 1** **Example:** `Device(config)# interface vlan 1`	Creates an interface and enters interface configuration mode.
Step 4	**ip address fe80::1 link-local** **Example:** `Device(config-if)# ip address 198.51.100.1 255.255.255.0`	Configures IPv6 address on the GigabitEthernet interface using the link-local option.

	Command or Action	Purpose
	Device(config-if)# **ipv6 address fe80::1 link-local** Device(config-if)# **ipv6 address 2001:DB8:0:1:FFFF:1234::5/64** Device(config-if)# **ipv6 address 2001:DB8:0:0:E000::F/64**	
Step 5	**ipv6 enable** **Example:** Device(config)# **ipv6 enable**	(Optional) Enables IPv6 on the GigabitEthernet interface.
Step 6	**no ipv6 nd managed-config-flag** **Example:** Device(config)# **interface vlan 1** Device(config-if)# **no ipv6 nd managed-config-flag**	Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.
Step 7	**no ipv6 nd other-config-flag** **Example:** Device(config-if)# **no ipv6 nd other-config-flag**	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 8	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Native IPv6

Information About IPv6

IPv6 is a packet-based protocol used to exchange data, voice, and video traffic over digital networks. IPv6 is based on IP, but with a much larger address space, and improvements such as a simplified main header and extension headers. The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while continuing to use services such as end-to-end security, quality of service (QoS), and globally unique addresses. The larger IPv6 address space allows networks to scale and provide global reachability.

Note The features and functions that work on IPv4 networks with IPv4 addresses also work on IPv6 networks with IPv6 addresses.

General Guidelines

- For IPv6 functionality to work, ensure that you disable IPv6 multicast routing.
- The Wireless Management interface should have only one static IPv6 address.

- Router advertisement should be suppressed on the wireless management interface and client VLANs (if IPv6 is configured on the client VLAN).
- Preferred mode is part of an AP join profile. When you configure the preferred mode as IPv6, an AP attempts to join over IPv6 first. If it fails, the AP falls back to IPv4.
- You should use MAC addresses for RA tracing of APs and clients.
- APs can join IPv6 controllers only with an IPv6 static address. If you have a controller with auto configurations and multiple IPv6 addresses, APs cannot join the IPv6 controllers.

Unsupported Features

- UDP Lite is not supported.
- AP sniffer over IPv6 is not supported.
- IPv6 is not supported for the HA port interface.
- Auto RF grouping over IPv6 is not supported. Only static RF grouping is supported.

Configuring IPv6 Addressing

Follow the procedure given below to configure IPv6 addressing:

Note All the features and functions that work on IPv4 networks with IPv4 addresses will work on IPv6 networks with IPv6 addresses too.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Configures IPv6 for unicasting.
Step 3	**interface vlan 1** **Example:** `Device(config)# interface vlan 1`	Creates an interface and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address* **Example:** `Device(config-if)# ipv6 address FD09:9:2:49::53/64`	Specifies a global IPv6 address.

	Command or Action	Purpose
Step 5	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 on the interface.
Step 6	**ipv6 nd ra suppress all** **Example:** `Device(config-if)# ipv6 nd ra suppress all`	Suppresses IPv6 router advertisement transmissions on the interface.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 8	**wireless management interface gigabitEthernet** *gigabitEthernet-interface-vlan 64* **Example:** `Device(config)# wireless management interface gigabitEthernet vlan 64`	Configures the ports that are connected to the supported APs with the wireless management interface.
Step 9	**ipv6 route** *ipv6-address* **Example:** `Device(config)# ipv6 route ::/0 FD09:9:2:49::1`	Specifies IPv6 static routes.

Creating an AP Join Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** window, click the **General** tab and click **Add**.

Step 3 In the **Name** field enter, a name for the AP join profile.

Step 4 (Optional) Enter a description for the AP join profile.

Step 5 Choose **CAPWAP** > **Advanced**.

Step 6 Under the **Advanced** tab, from the **Preferred Mode** drop-down list, choose **IPv6**. This sets the preferred mode of APs as IPv6.

Step 7 Click **Save & Apply to Device**.

Creating an AP Join Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**description** *ap-profile-name* **Example:** `Device(config-ap-profile)# description "xyz ap profile"`	Adds a description for the AP profile.
Step 4	**preferred-mode ipv6** **Example:** `Device(config-ap-profile)# preferred-mode ipv6`	Sets the preferred mode of APs as IPv6.

Configuring the Primary and Backup Controller (GUI)

Before you begin

Ensure that you have configured an AP join profile prior to configuring the primary and backup controller s.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 On the **AP Join Profile** window, click the AP join profile name.

Step 3 In the **Edit AP Join Profile** window, click the **CAPWAP** tab.

Step 4 In the **High Availability** tab, under **Backup Controller Configuration**, check the **Enable Fallback** check box.

Step 5 Enter the primary and secondary controller names and IP addresses.

Step 6 Click **Update & Apply to Device**.

Configuring Primary and Backup Controller (CLI)

Follow the procedure given below to configure the primary and secondary controllers for a selected AP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile yy-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**capwap backup primary** *primary-controller-name primary-controller-ip* **Example:** `Device(config)# capwap backup primary WLAN-Controller-A 2001:DB8:1::1`	Configures AP CAPWAP parameters with the primary backup controller's name. **Note** You need to enable fast heartbeat for **capwap backup primary** and **capwap backup secondary** to work. AP disconnection may occur if the link between the controller and AP is not reliable and fast heartbeat is enabled.
Step 4	**ap capwap backup secondary** *secondary-controller-name secondary-controller-ip* **Example:** `Device(config)# capwap backup secondary WLAN-Controller-B 2001:DB8:1::1`	Configures AP CAPWAP parameters with the secondary backup controller's name.
Step 5	**syslog host** *ipaddress* **Example:** `Device(config)# syslog host 2001:DB8:1::1`	Configures the system logging settings for the APs.
Step 6	**tftp-downgrade** *tftp-server-ip imagename* **Example:** `Device(config)# tftp-downgrade 2001:DB8:1::1 testimage`	Initiates AP image downgrade from a TFTP server for all the APs.

Verifying IPv6 Configuration

Use the following **show** command to verify the IPv6 configuration:

```
Device# show wireless interface summary

Wireless Interface Summary
```

```
Interface Name Interface Type VLAN ID IP Address      IP Netmask     MAC Address
-------------------------------------------------------------------------------------
Vlan49         Management     49      0.0.0.0       255.255.255.0    001e.f64c.1eff
                                      fd09:9:2:49::54/64
```

CHAPTER 146

IPv6 ACL

- Information About IPv6 ACL, on page 1601
- Prerequisites for Configuring IPv6 ACL, on page 1602
- Restrictions for Configuring IPv6 ACL, on page 1602
- Configuring IPv6 ACLs , on page 1602
- How To Configure an IPv6 ACL, on page 1603
- Verifying IPv6 ACL, on page 1608
- Configuration Examples for IPv6 ACL, on page 1609

Information About IPv6 ACL

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs are configured on the device and applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU.

You can also create a preauthentication ACL for web authentication. Such an ACL is used to allow certain types of traffic before authentication is complete.

IPv6 ACLs support the same options as IPv4 ACLs including source, destination, source and destination ports.

Note You can enable only IPv4 traffic in your network by blocking IPv6 traffic. That is, you can configure an IPv6 ACL to deny all IPv6 traffic and apply it on specific or all WLANs.

Understanding IPv6 ACLs

Types of ACL

Per User IPv6 ACL

For the per-user ACL, the full access control entries (ACE) as the text strings are configured on the RADIUS server.

The ACE is not configured on the Cisco 9800 controller. The ACE is sent to the device in the `ACCESS-Accept` attribute and applies it directly for the client. When a wireless client roams into an foreign device, the ACEs are sent to the foreign device as an AAA attribute in the mobility Handoff message. Output direction, using per-user ACL is not supported.

Filter ID IPv6 ACL

For the filter-Id ACL, the full ACEs and the `acl name(filter-id)` is configured on the Cisco 9800 controller and only the `filter-id` is configured on the RADIUS Server.

The `filter-id` is sent to the device in the ACCESS-Accept attribute, and the device looks up the filter-id for the ACEs, and then applies the ACEs to the client. When the client L2 roams to the foreign device, only the filter-id is sent to the foreign device in the mobility Handoff message. Output filtered ACL, using per-user ACL is not supported. The foreign device has to configure the filter-id and ACEs beforehand.

Prerequisites for Configuring IPv6 ACL

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP Version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic when the switch is running the Network Essentials license.

Restrictions for Configuring IPv6 ACL

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs. The IPv6 ACL does not support Flex connect mode.

The device supports most of the Cisco IOS-supported IPv6 ACLs with some exceptions:

- The device does not support matching on these keywords: **flowlabel**, **routing header**, and **undetermined-transport**.
- The device does not support reflexive ACLs (the **reflect** keyword).
- The device does not apply MAC-based ACLs on IPv6 frames.
- When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the device checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.
- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the device does not allow the ACE to be added to the ACL that is currently attached to the interface

Configuring IPv6 ACLs

Follow the procedure given below to filter IPv6 traffic:

1. Create an IPv6 ACL, and enter IPv6 access list configuration mode.

2. Configure the IPv6 ACL to block (deny) or pass (permit) traffic.
3. Apply the IPv6 ACL to the interface where the traffic needs to be filtered.
4. Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied.

Default IPv6 ACL Configuration

There are no IPv6 ACLs configured or applied.

Interaction with Other Features and Switches

- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

  You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the hardware memory is full, for any additional configured ACLs, packets are processed to the CPU, and the ACLs are applied in software. When the hardware is full a message is printed to the console indicating the ACL has been unloaded and the packets will be processed in software.

Note Only packets of the same type as the ACL that could not be added (ipv4, ipv6, MAC) will be processed in software.

- If the TCAM is full, for any additional configured ACLs, packets are forwarded to the CPU, and the ACLs are applied in software.

How To Configure an IPv6 ACL

Creating an IPv6 ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** dialog box, enter the following parameters.

- **ACL Name:** Enter the name for the ACL
- **ACL Type:** IPv6
- **Sequence:** The valid range is between 100 and 199 or 2000 and 26991
- **Action:** Choose **Permit** or **Deny** the packet flow from the drop-down list.
- **Source Type:** Choose **any**, **Host** or **Network** from which the packet is sent.
- **Destination Type:** Choose **any**, **Host** or **Network** to which the packet is sent.
- **Protocol:** Choose a protocol from the drop-down list.
- **Log:** Enable or disable logging.
- **DSCP:** Enter to match packets with the DSCP value

Step 4 Click **Add**.

Step 5 Add the rest of the rules and click **Apply to Device**.

Creating an IPv6 ACL

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *acl_name* **Example:** `Device# ipv6 access-list access-list-name`	Use a name to define an IPv6 access list and enter IPv6 access-list configuration mode.
Step 4	**{deny|permit} protocol** **Example:** `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length`	Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions: • For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer

	Command or Action	Purpose
	`| any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	in the range 0 to 255 representing an IPv6 protocol number. • The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). • Enter any as an abbreviation for the IPv6 prefix ::/0. • For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons. • (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range. If the operator follows the source-ipv6-prefix/prefix-length argument, it must match the source port. If the operator follows the destination-ipv6-prefix/prefix-length argument, it must match the destination port. • (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP. • (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63. • (Optional) For packet fragmentation, enter fragments to check noninitial

	Command or Action	Purpose
		fragments. This keyword is visible only if the protocol is ipv6. • (Optional) Enter log to cause an logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs. • (Optional) Enter routing to specify that IPv6 packets be routed. • (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295 • (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.
Step 5	**{deny|permit} tcp** **Example:** `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	(Optional) Define a TCP access list and the access conditions. Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3, with these additional optional parameters: • ack—Acknowledgment bit set. • established—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set. • fin—Finished bit set; no more data from sender. • neq {port | protocol}—Matches only packets that are not on a given port number. • psh—Push function bit set. • range {port | protocol}—Matches only packets in the port number range. • rst—Reset bit set. • syn—Synchronize bit set. • urg—Urgent pointer bit set.

	Command or Action	Purpose
Step 6	**{deny|permit} udp** **Example:** `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port |protocol}] [range {port |protocol}] [routing][sequence value][time-range name]`	(Optional) Define a UDP access list and the access conditions. Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the operator [port]] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.
Step 7	**{deny|permit} icmp** **Example:** `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]`	(Optional) Define an ICMP access list and the access conditions. Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings: • icmp-type—Enter to filter by ICMP message type, a number from 0 to 255. • icmp-code—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • icmp-message—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release.
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 9	**show ipv6 access-list** **Example:** `show ipv6 access-list`	Verify the access list configuration.
Step 10	**copy running-config startup-config** **Example:** `copy running-config startup-config`	(Optional) Save your entries in the configuration file.

Creating WLAN IPv6 ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer3** tab, click **Show Advanced Settings** and under the **Preauthenticated ACL** settings, choose the ACL from the **IPv6** drop-down list.

Step 5 Click **Apply to Device**.

Creating WLAN IPv6 ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `DeviceController # configure terminal`	Configures the terminal.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy test1`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**ipv6 acl** *acl_name* **Example:** `Device(config-wireless-policy)# ipv6 acl testacl`	Creates a named WLAN ACL.
Step 4	**ipv6 traffic-filter web** *acl_name-preauth* **Example:** `Device(config-wlan)# ipv6 traffic-filter web preauth1`	Creates a pre-authentication ACL for web authentication.

Verifying IPv6 ACL

Displaying IPv6 ACLs

To display IPv6 ACLs, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**show access-list** **Example:** `Device# show access-lists`	Displays all access lists configured on the device
Step 4	**show ipv6 access-list** *acl_name* **Example:** `Device# show ipv6 access-list [access-list-name]`	Displays all configured IPv6 access list or the access list specified by name.

Configuration Examples for IPv6 ACL

Example: Creating an IPv6 ACL

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic. The second permit entry is necessary because an implicit deny -all condition is at the end of each IPv6 access list.

Note Logging is supported only on Layer 3 interfaces.

```
Device(config)# ipv6 access-list CISCO
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(config-ipv6-acl)# permit any any
```

Example: Applying an IPv6 ACL to a Policy Profile in a Wireless Environment

This example shows how to apply an IPv6 ACL to a Policy Profile in a Wireless environment.

Note All IPv6 ACLs must be associated to a policy profile.

1. Creating an IPv6 ACL.

```
Device(config)# ipv6 access-list <acl-name>
Device(config-ipv6-acl)# permit tcp 2001:DB8::/32 any
Device(config-ipv6-acl)# permit udp 2001:DB8::/32 any
```

2. Applying the IPv6 ACL to a policy profile.

```
Device(config)# wireless profile policy <policy-profile-name>
Device(config-wireless-policy)# shutdown
Device(config-wireless-policy)# ipv6 acl <acl-name>
Device(config-wireless-policy)# no shutdown
```

Displaying IPv6 ACLs

To display IPv6 ACLs, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**show access-list** **Example:** `Device# show access-lists`	Displays all access lists configured on the device
Step 2	**show ipv6 access-list** *acl_name* **Example:** `Device# show ipv6 access-list [access-list-name]`	Displays all configured IPv6 access list or the access list specified by name.

Example: Displaying IPv6 ACLs

This is an example of the output from the **show access-lists** privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

```
Device #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

This is an example of the output from the **show ipv6 access-lists** privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack.

```
Device# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
```

```
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

Example: Configuring RA Throttling

This task describes how to create an RA throttle policy in order to help the power-saving wireless clients from being disturbed by frequent unsolicited periodic RA's. The unsolicited multicast RA is throttled by the controller.

Before you begin

Enable IPv6 on the client machine.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ipv6 nd ra-throttler policy Mythrottle** **Example:** `Device (config)# ipv6 nd ra-throttler policy Mythrottle`	Creates a RA throttler policy called Mythrottle.
Step 3	**throttle-period 20** **Example:** `Device (config-nd-ra-throttle)# throttle-period 20`	Determines the time interval segment during which throttling applies.
Step 4	**max-through 5** **Example:** `Device (config-nd-ra-throttle)# max-through 5`	Determines how many initial RA's are allowed.
Step 5	**allow at-least 3 at-most 5** **Example:** `Device (config-nd-ra-throttle)# allow at-least 3 at-most 5`	Determines how many RA's are allowed after the initial RAs have been transmitted, until the end of the interval segment.
Step 6	**switch (config)# vlan configuration 100** **Example:** `Device (config)# vlan configuration 100`	Creates a per vlan configuration.
Step 7	**ipv6 nd ra-th attach-policy attach-policy_name** **Example:**	Enables the router advertisement throttling.

	Command or Action	Purpose
	`Device (config)# ipv6 nd ra-throttle attach-policy attach-policy_name`	
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

CHAPTER 147

IPv6 Client Mobility

- Information About IPv6 Client Mobility, on page 1613
- Prerequisites for IPv6 Client Mobility, on page 1615
- Monitoring IPv6 Client Mobility, on page 1616

Information About IPv6 Client Mobility

Link layer mobility is not enough to make wireless client Layer 3 applications continue to work seamlessly while roaming. Cisco IOSd's wireless mobility module uses mobility tunneling to retain seamless connectivity for the client's Layer 3 PoP (point of presence) when the client roams across different subnets on different switches.

IPv6 is the next-generation network layer Internet protocol intended to replace IPv4 in the TCP/IP suite of protocols. This new version increases the internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, which provide significantly more addresses than the 32-bit IPv4 addresses.

To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network. The device keeps track of IPv6 clients by intercepting the ICMPv6 messages to provide seamless mobility and protect the network from network attacks. The NDP (neighbor discovery packets) packets are converted from multicast to unicast and delivered individually per client. This unique solution ensures that Neighbor Discovery and Router Advertisement packets are not leaked across VLANs. Clients can receive specific Neighbor Discovery and Router Advertisement packets ensuring correct IPv6 addressing to avoid unnecessary multicast traffic.

The configuration for IPv6 mobility is the same as IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The device must be part of the same mobility group. Both IPv4 and IPv6 client mobility are enabled by default.

IPv6 client mobility is used for the following:

- Retaining the client IPv6 multiple addresses in Layer-2 and Layer-3 roaming.
- IPv6 Neighbor Discovery Protocol (NDP) packet management.
- Client IPv6 addresses learning.

Note The configuration for IPv6 mobility in SDA wireless and Local mode is the same as of IPv4 mobility and requires no different software configuration on the client side to achieve seamless roaming. Refer to IPv4 mobility section for configuration information.

Note If ipv6 address is configured on the SVI, you should configure **ipv6 nd ra suppress all** command on all client VLAN SVI interfaces on the controller. This prevents multiple devices from advertising themselves as the routers.

Using Router Advertisement

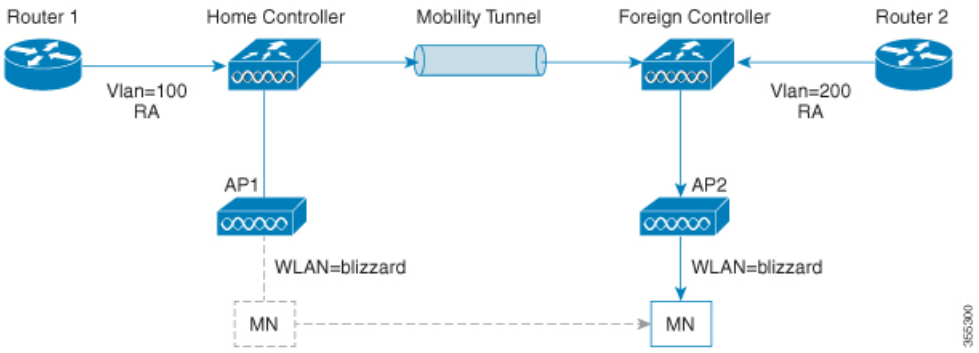
The Neighbor Discovery Protocol (NDP) operates in the link-layer and is responsible for the discovery of other nodes on the link. It determines the link-layer addresses of other nodes, finds the available routers, and maintains reachability information about the paths to other active neighbor nodes.

Router Advertisement (RA) is one of the IPv6 Neighbor Discovery Protocol (NDP) packets that is used by the hosts to discover available routers, acquire the network prefix to generate the IPv6 addresses, link MTU, and so on. The routers send RA on a regular basis, or in response to hosts Router Solicitation messages.

IPv6 wireless client mobility manages the IPv6 RA packet . The device forwards the link-local all-nodes multicast RA packets to the local and roaming wireless nodes mapped on same VLAN the RA was received on.

Figure 1 illustrates how a roaming client “MN” receives RA from VLAN 200 in a foreign controller and how it acquires an new IP address and breaks into L3 mobility's point of presence.

Figure 49: Roaming Client Receives Valid RA from Router 1



Router Advertisement Throttling

RA throttling allows the controller to enforce limits to the RA packets headed toward the wireless network. By enabling RA throttling, routers that send multiple RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicast to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

IPv6 Address Learning

There are three ways for IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLAAC)
- Stateful DHCPv6
- Static configuration

For these methods, the IPv6 client always sends NS DAD (duplicate address detection) to ensure that there is no duplicated IP address on the network. The device snoops the clients NDP and DHCPv6 packets to learn about its client IP addresses and then updates the controllers database. The database then informs the controller for the clients new IP address.

Handling Multiple IP Addresses

In the case when the new IP address is received after RUN state, whether an addition or removal, the controller updates the new IP addresses on its local database for display purposes. Essentially, the IPv6 uses the existing or same PEM state machine code flow as in IPv4. When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller will include all the available IP addresses, IPv4 and IPv6, in the API/SPI interface to the external entities.

An IPv6 client can acquire multiple IP addresses from stack for different purposes. For example, a link-local address for link local traffic, and a routable unique local or global address.

When the client is in the DHCP request state and the controller receives the first IP address notification from the database for either an IPv4 or IPv6 address, the PEM moves the client into the RUN state.

When a new IP address is received after the RUN state, either for addition or removal, the controller updates the new IP addresses on its local database for display purposes.

When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller provides the available IP addresses, both IPv4 and IPv6, to the external entities.

IPv6 Configuration

The device supports IPv6 client as seamlessly as the IPv4 clients. The administrator must manually configure the VLANs to enable the IPv6, IPv6's snooping and throttling functionality. This will enable the NDP packets to throttle between the device and its various clients.

Prerequisites for IPv6 Client Mobility

- To enable wireless IPv6 client connectivity, the underlying wired network must support IPv6 routing and an address assignment mechanism such as SLAAC or DHCPv6. The device must have L2 adjacency to the IPv6 router, and the VLAN needs to be tagged when the packets enter the device. APs do not require connectivity on an IPv6 network, as all traffic is encapsulated inside the IPv4 CAPWAP tunnel between the AP and device.
- When using the IPv6 Client Mobility, clients must support IPv6 with either static stateless auto configuration or stateful DHCPv6 IP addressing .

- To allow smooth operation of stateful DHCPv6 IP addressing, you must have a switch or router that supports the DHCP for IPv6 feature that is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

Monitoring IPv6 Client Mobility

The commands in Table 1 are used to monitor IPv6 Client mobility on the device.

Table 120: Monitoring IPv6 Client Mobility Commands

Commands	Description
show wireless client summary	Displays the wireless specific configuration of active clients.
show wireless client mac-address `(mac-addr-detail)`	Displays the wireless specific configuration of active clients based on their MAC address.

CHAPTER 148

IPv6 Support on Flex and Mesh

- IPv6 Support on Flex + Mesh Deployment, on page 1617
- Configuring IPv6 Support for Flex + Mesh, on page 1617
- Verifying IPv6 on Flex+Mesh , on page 1619

IPv6 Support on Flex + Mesh Deployment

IPv6 is the backhaul transport of the Service Provider. The IPv6 support over flex + mesh feature is now supported on the Cisco Catalyst 9800 Series Wireless Controller . WLAN accepts IPv6 clients and forward the traffic.

Configuring IPv6 Support for Flex + Mesh

Follow the procedure given below to enable the IPv6 routing on the controller :

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-interface-number* **Example:** `Device(config)#interface vlan 89`	Creates an interface and enters the interface configuration mode.
Step 3	**shutdown** **Example:** `Device(config-if)#shutdown`	Disables the interface configuration.
Step 4	**ipv6 enable** **Example:** `Device(config-if)#ipv6 enable`	Optional. Enables IPv6 on the interface.

	Command or Action	Purpose
Step 5	**ipv6 address** *X:X:X:X::X/<0-128>* **Example:** `Device(config-if)#ipv6 address 1:1:1:1::1/64`	Configures IPv6 address on the interface using the IPv6 prefix option.
Step 6	**no shutdown** **Example:** `Device(config-if)#no shutdown`	Enables the IPv6 address.
Step 7	**no shutdown** **Example:** `Device(config-if)#no shutdown`	Enables the PIM dense-mode operation.
Step 8	**end** **Example:** `Device(config-if)#end`	Returns to privileged EXEC mode.
Step 9	**show ipv6 interface brief** **Example:** `Device#show ipv6 interface brief`	Verifies your entries.
Step 10	**ping ipv6** *destination-address or hostname* **Example:** `Device#ping ipv6 1:1:1:1::10`	Checks the gateway connectivity.

Configuring Preferred IP Address as IPv6 (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click the AP Join Profile Name. The **Edit AP Join Profile** window is displayed.

Step 3 Choose **CAPWAP** > **Advanced**.

Step 4 From the **Preferred Mode** drop-down list, select **IPV6**.

Step 5 Click **Update & Apply to Device**.

Configuring Preferred IP Address as IPv6

Procedure

	Command or Action	Purpose
Step 1	**Configure Terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *default-ap-profile* **Example:** `Device(config)# ap profile default-ap-profile`	Enters AP profile configuration mode.
Step 3	**preferred-mode ipv6** **Example:** `Device(config-ap-profile)# preferred-mode ipv6`	Uses IPv6 to join the controller .
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits the configuration mode and returns to privileged EXEC mode.

Verifying IPv6 on Flex+Mesh

To verify the IPv6 configuration on the controller , use the following **show** command:

```
Device#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet2       unassigned      YES unset  up                    up
GigabitEthernet0       unassigned      YES NVRAM  administratively down down
Capwap1                unassigned      YES unset  up                    up
Capwap2                unassigned      YES unset  up                    up
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan89                 9.10.89.90      YES NVRAM  up                    up
Ewlc-9.10.89.90#show running-config interface vlan 89
Building configuration...

Current configuration : 120 bytes
!
interface Vlan89
 ip address 9.10.89.90 255.255.255.0
 ip helper-address 9.1.0.100
 no mop enabled
 no mop sysid
end
```

CHAPTER 149

IPv6 CAPWAP UDP Lite Support

- Information About UDP Lite, on page 1621
- Enabling UDP Lite Support, on page 1621
- Verifying UDP Lite Support Configuration, on page 1622

Information About UDP Lite

The UDP Lite Support feature, which is an enhancement to the existing IPv6 functionality, supports the UDP Lite protocol.

This feature is only applicable to the IPv6 addresses of the controller and APs. IPv6 mandates complete payload checksum for UDP. The UDP Lite Support feature minimizes the performance impact on the controller and AP by restricting the checksum calculation coverage for the UDP Lite header to 8 bytes only.

The use of the UDP Lite Support feature impacts intermediate firewalls to allow UDP Lite protocol (protocol ID of 136) packets. Existing firewalls might not provide the option to open specific ports on UDP Lite protocol. In such cases, the administrator must open up all the ports on UDP Lite.

Restrictions for UDP Lite Support

- Mobility IPv6 tunnels do not support the UDP Lite Support feature.

Enabling UDP Lite Support

The following procedure describes the steps involved in enabling UDP Lite for an AP profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:**	Configures an AP profile and enters AP profile configuration mode.

	Command or Action	Purpose
	`Device(config)# ap profile default-ap-profile`	
Step 3	**capwap udplite** **Example:** `Device(config-ap-profile)# capwap udplite`	Enables IPv6 CAPWAP UDP Lite on the AP. **Note** The following message is displayed after the configuration: `This feature is supported only for IPv6 data packets, APs will be rebooted.`
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying UDP Lite Support Configuration

To verify the CAPWAP UDP Lite status, use the following command:

```
Device# show ap profile name default-ap-profile detailed
CAPWAP UDP-Lite                 : ENABLED
Lawful-Interception             : ENABLED
  LI timer                      : 60
AWIPS                           : DISABLED
AWIPS Forensic                  : Unknown
Client RSSI Statistics
  Reporting                     : ENABLED
  Reporting Interval            : 30 seconds
```

CHAPTER 150

Neighbor Discovery Proxy

- Information About Neighbor Discovery, on page 1623
- Configure Neighbor Discovery Proxy (CLI), on page 1623
- Configure Duplicate Address Detection Proxy (CLI), on page 1624

Information About Neighbor Discovery

In IPv6 networks, Neighbor Discovery Protocol (NDP) uses ICMPv6 messages and solicited-node multicast addresses to track and discover the other IPv6 hosts present on the other side of connected interfaces. As part of this process, a host queries for other node link-layer addresses to verify neighbor reachability using Neighbor Solicitation (NS) messages. In response to the NS messages, a Neighbor Advertisement (NA) is sent to provide information to neighbors.

Configure Neighbor Discovery Proxy (CLI)

Neighbor Discovery (ND) Proxy is the ability of the controller to respond to the Neighbor Solicitation packet destined for wireless clients. During Neighbor Discovery suppression, the controller checks if proxy is enabled for the destined wireless clients. If proxy is enabled, the controller drops the Neighbor Solicitation packet and generates a response to the Neighbor Solicitation source in such a way that the packet appears to be coming from a wireless client. This helps in limiting the traffic to the wireless clients.

If Neighbor Discovery Proxy is not enabled, the multicast Neighbor Solicitation is converted into unicast Neighbor Solicitation with the MAC address of the target client and is forwarded to that client.

Note

- Neighbor Discovery proxy is applicable only in central switching mode.
- A controller does not proxy the Neighbor Solicitation packet if the destination address is not that of a wireless client.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**ipv6 nd proxy full-proxy** **Example:** `Device(config-wireless-policy)# ipv6 nd proxy full-proxy`	Enables ND proxy.

Configure Duplicate Address Detection Proxy (CLI)

The IPv6 Duplicate Address Detection (DAD) feature ensures that all the IP addresses assigned on a particular segment are unique. A proxy is required to ensure that multicast and unicast packets are not sent towards the wireless device for which it is enabled.

DAD verifies whether the host address is unique. The IPv6 DAD Proxy feature responds on behalf of the address owner when an address is in use.

However, in a scenario where nodes are restricted from talking to each other at Layer 2, DAD cannot detect a duplicate address. If DAD proxy is disabled, the multicast packet is converted into unicast and is sent to the target client.

Note

- DAD proxy is applicable only in central switching mode.
- A controller does not proxy the DAD NS packet if the destination address is not that of a wireless client.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 nd proxy dad-proxy** **Example:** `Device(config-wireless-policy)# ipv6 nd proxy dad-proxy`	Enables DAD proxy. **Note** Full proxy configuration is a superset of ND proxy and DAD proxy configuration. Hence, use the **ipv6 nd proxy full-proxy** command also to enable DAD proxy.

CHAPTER 151

Address Resolution Protocol Proxy

- Information About Address Resolution Protocol, on page 1627
- Configure Address Resolution Protocol Proxy (CLI), on page 1627

Information About Address Resolution Protocol

The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP) [RFC826], specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. When a wireless client sends an ARP request for an IP address of interest, the controller performs a search for that address in its database. If an entry is found in the controller database, then the ARP is converted to unicast and forwarded to that particular client. If there is no entry in the controller's database, the ARP request is flooded out to the VLAN wired ports.

Configure Address Resolution Protocol Proxy (CLI)

ARP Proxy is the ability of the controller to respond to the ARP request packet destined for the wireless clients. During broadcast suppression, the controller checks if proxy is enabled for the destined wireless clients. If proxy is enabled, the controller drops the ARP request packet and generates a response to the source of the ARP request in a way that the packet appears to be coming from the wireless client. This helps in limiting the traffic to the wireless clients.

If ARP Proxy is not enabled, the broadcast ARP request is converted into an unicast ARP request with the MAC address of the target client, and is forwarded to only that client.

Note

- Proxy ARP is applicable only in central switching mode.
- A device will not proxy the ARP request if the destination address is not that of a wireless client.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**ipv4 arp-proxy** **Example:** `Device(config-wireless-policy)# ipv4 arp-proxy`	Enables ARP proxy.

CHAPTER 152

IPv6 Ready Certification

- Feature History for IPv6-Ready Certification, on page 1629
- IPv6 Ready Certification, on page 1629
- Configuring IPv6 Route Information, on page 1630
- Verifying IPv6 Route Information, on page 1630

Feature History for IPv6-Ready Certification

This table provides release and related information for the feature explained in this module.

This feature is available in all the releases subsequent to the one in which it is introduced in, unless noted otherwise.

Table 121: Feature History for IPv6-Ready Certification

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.6.1	IPv6-Ready Certification	This feature is enhanced with the implementation of various IPv6 functionalities that are required to comply with the latest RFC specifications.

IPv6 Ready Certification

Cisco IOS XE Bengaluru, 17.6.1 has implemented various IPv6 functionalities that are required for compliance with the latest RFC specifications for IPv6 Ready Certification. The newly implemented IPv6 functionalities are:

- **Fragment Processing and Reassembly (RFC8200)**: The first fragment must contain the mandatory extension header up to the first upper level protocol (ULP) header as specified in RFC 8200.
- **Handling Atomic Fragments in Neighbor Discovery (RFC6980)**: Fragmented neighbor discovery packets must be dropped.
- **Packet too Big (RFC8201)**: Atomic fragmentation is not supported. Packets failing to meet the IPv6 MTU requirement of 1280 are dropped.

- **Route Information Options (RIO) in IPv6 Router Advertisements (RFC4191)**: A new RIO is added to the IPv6 Router Advertisement message for communicating specific routes from routers to hosts. Explicit route configuration ensures that only necessary routes are advertised to the hosts.
- **IPv6 Hop-by-Hop Processing (RFC 8200)**: This enhancement allows explicit configuration of the nodes, along the delivery path of the packets that require hop-by-hop options header processing.

Configuring IPv6 Route Information

The Route Information Option (RIO) in the IPv6 router advertisement messages helps in communicating specific routes from routers to hosts. This improves a host's ability to pick up an appropriate default router, when the host is multihomed and the routers are on different links. The explicit route configuration ensures that only necessary routes are advertised to the hosts.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface* **Example:** `Device(config)# interface gigabitethernet1.1`	Specifies the interface and enters interface configuration mode.
Step 3	**ipv6 nd ra specific-route** *prefix/length* **lifetime** *lifetime/infinity* [**preference** *preference*] **Example:** `Device(config-if)# ipv6 nd ra specific-route 3::3/116 lifetime 11 preference medium`	Configures RIO in IPv6 router advertisement messages. For more information, see the ipv6 nd ra specific route command.

Verifying IPv6 Route Information

To identify the specific routes that are sent in the router advertisements, use the following command:

```
Device# show ipv6 nd ra specific-route

IPv6 Prefix/Length Lifetime Preference Interface
---------------------------------------- -------- ---------- ---------
1234::12/127 1000 High GigabitEthernet2
```

PART XII

CleanAir

- Cisco CleanAir, on page 1633
- Bluetooth Low Energy, on page 1653
- Persistent Device Avoidance, on page 1657
- Spectrum Intelligence, on page 1661
- Spectrum Analysis, on page 1665

CHAPTER 153

Cisco CleanAir

- Feature History for CleanAir, on page 1633
- Information About Cisco CleanAir, on page 1633
- Prerequisites for CleanAir, on page 1637
- Restrictions for CleanAir, on page 1637
- How to Configure CleanAir, on page 1638
- CleanAir Pro Scanning, on page 1645
- Verifying CleanAir Parameters, on page 1649
- Configuration Examples for CleanAir, on page 1650
- CleanAir FAQs, on page 1651

Feature History for CleanAir

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 122: Feature History for CleanAir

Release	Feature	Feature Information
Cisco IOS XE 17.13.1	EDRRM Support for 6-GHz Band Radio	The Event-Driven Radio Resource Management (EDRRM) is enabled in 6-GHz band radio of AP.

Information About Cisco CleanAir

Cisco CleanAir is a solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all the users of a shared spectrum (both native devices and foreign interferers). It also enables the network to act upon this information. For example, you can manually remove the interfering device, or the system can automatically change the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points and Cisco Catalyst 9800 Series Wireless Controller . These access points collect information about all the devices that operate in the industrial, scientific,

and medical (ISM) bands, identify and evaluate the information as a potential interference source, and forward it to the controller . The controller controls the access points and displays the interference devices.

For every device operating in the unlicensed band, Cisco CleanAir provides information about what it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF so that you do not have to be an RF expert.

Wireless LAN systems operate in unlicensed 2.4-GHz and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect the Wi-Fi operations.

Some of the most advanced WLAN services, such as voice-over-wireless and IEEE 802.11 radio communications, might be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality addresses this problem of RF interference.

Cisco CleanAir-Related Terms

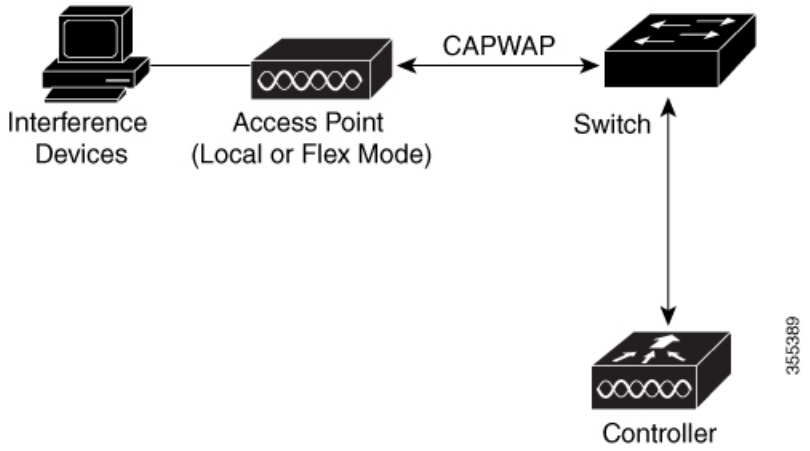
Table 123: CleanAir-Related Terms

Term	Description
AQI	Air Quality Index. The AQI is an indicator of air quality, based on the RF interferences. An AQI of 0 is bad and an AQI > 85 is good.
AQR	Air Quality Report. AQRs contain information about total interference from all the identified sources represented by AQI and the summary of the most severe interference categories. AQRs are sent every 15 minutes to the Mobility Controller and every 30 seconds in the Rapid mode.
DC	Duty Cycle. Percentage of time that the channel is utilized by a device.
EDRRM	Event-Driven RRM. EDRRM allows an access point in distress to bypass normal RRM intervals and immediately change channels.
IDR	Interference Device Reports that an access point sends to the controller .
ISI	Interference Severity Index. The ISI is an indicator of the severity of the interference.
RSSI	Received Signal Strength Indicator. RSSI is a measurement of the power present in a received radio signal. It is the power at which an access point sees the interferer device.

Cisco CleanAir Components

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and device.

Figure 50: Cisco CleanAir Solution



An access point equipped with Cisco CleanAir technology collects information about Wi-Fi interference sources and processes it. The access point collects and sends the Air Quality Report (AQR) and Interference Device Report (IDR) to the controller .

The controller controls and configures CleanAir-capable access points, and collects and processes spectrum data. The controller provides local user interfaces (GUI and CLI) to configure basic CleanAir features and services and display current spectrum information. The controller also detects, merges, and mitigates interference devices using RRM TPC and DCA For details, see Interference Device Merging.

The device performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (GUI and CLI) for configuring Cisco CleanAir features and retrieving data.
- Displays spectrum data.
- Collects and processes AQRs from the access point and stores them in the air quality database. AQRs contain information about the total interference from all the identified sources represented by the Air Quality Index (AQI) and the summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per-interference type reports that enable you to take action in scenarios where interference because of unclassified interfering devices is more.
- Collects and processes IDRs from the access point and stores them in the interference device database.

Note When Cisco CleanAir is disabled and Spectrum Intelligence (SI) is enabled in the controller, both CleanAir and Air Quality reporting are disabled. In spite of this, Air Quality is still populated for SI APs and viewed as disabled when **show ap dot11 5ghz/24ghz cleanair config** command is executed. This is an expected behavior as SI APs report Air Quality.

Here, Spectrum intelligence is a subset of CleanAir features. For more information on Spectrum Intelligence, see the *Spectrum Intelligence Deployment Guide*.

Interference Types that Cisco CleanAir can Detect

Cisco CleanAir access points can detect and report severity of the interference. Spectrum event-driven RRM is one such mitigation strategy.

Wi-Fi chip-based RF management systems share these characteristics:

- Any RF energy that cannot be identified as a Wi-Fi signal is reported as noise.
- Noise measurements that are used to assign a channel plan tend to be averaged over a period of time to avoid instability or rapid changes that can be disruptive to certain client devices.
- Averaging measurements reduces the resolution of the measurement. As such, a signal that disrupts clients might not look like it needs to be mitigated after averaging.
- All RF management systems available today are reactive in nature.

Cisco CleanAir is different and can positively identify not only the source of the noise but also its potential impact to a WLAN. Having this information allows you to consider the noise within the context of the network and make intelligent and, where possible, proactive decisions. Spontaneous interference event is commonly used for CleanAir.

Note Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) which, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

Microwave Ovens, Outdoor Ethernet bridges are two classes of devices that qualify as persistent, since once detected, it is likely that these devices will continue to be a random problem and are not likely to move. For these types of devices we can tell RRM of the detection and Bias the affected channel so that RRM "remembers" that there is a high potential for client impacting interference for the Detecting AP on the detected channel. For more information, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper_chapter_0100.html?bookSearch=true#id_15217.

CleanAir PDA devices include:

- Microwave Oven
- WiMax Fixed
- WiMax Mobile
- Motorola Canopy

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interference only if the devices are actively transmitting. Bluetooth devices have extensive power-save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

EDRRM and AQR Update Mode

EDRRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AQ and reports the AQ every 15 minutes. AQ only reports classified interference devices. The key benefit of EDRRM is fast action time. If an interfering device is operating on an active channel and causes enough AQ degradation to trigger an EDRRM, then no clients will be able to use that channel or the access point. You must remove the access point from the channel. EDRRM is not enabled by default, you must first enable CleanAir and then enable EDRRM.

Prerequisites for CleanAir

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Only Cisco CleanAir-enabled access points using the following access point modes can perform Cisco CleanAir spectrum monitoring:

- Local—In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only. An AP can only measure air quality and interference when the AP is not busy transmitting Wi-Fi frames. This implies that CleanAir detections will be drastically lower if the AP is having a high channel utilization.
- FlexConnect—When a FlexConnect access point is connected to the controller , its Cisco CleanAir functionality is identical to local mode.
- Monitor—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

  The following options are available:

  - All—All channels
  - DCA—Channel selection governed by the DCA list
  - Country—All channels are legal within a regulatory domain

Restrictions for CleanAir

- Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor access point list. IDR clustering depends on the device's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- For 4800 AP slot 1 5 GHz is dedicated and cannot be individually moved to monitor mode. However, slot 0 is XOR and can be moved to monitor as well as 2.4/5 GHz. Slot 2 is dedicated monitor and will operate in 5GHz and in AP monitor mode, slot 2 will be disabled because a monitor radio is already available in both 2.4/5GHz. 3700 AP has dedicated 2.4GHz (slot0) and 5GHz (slot1).
- Do not connect access points in SE connect mode directly to any physical port on the controller.
- CleanAir is not supported wherein the channel width is 160 MHz.

How to Configure CleanAir

Enabling CleanAir for the 2.4-GHz Band (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**

Step 2 On the **CleanAir** page, click the me**2.4 GHz Band** > **General** tab.

Step 3 Check the **Enable CleanAir** checkbox.

Step 4 Click **Apply**.

Enabling CleanAir for the 2.4-GHz Band (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 24ghz cleanair**
	Example:
	`Device(config)#ap dot11 24ghz cleanair`
	`Device(config)#no ap dot11 24ghz cleanair`
		Enables the CleanAir feature on the 802.11b network. Run the **no** form of this command to disable CleanAir on the 802.11b network.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Interference Reporting for a 2.4-GHz Device (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**.

Step 2 Click the **2.4 GHz Band** tab.

Step 3 Choose the interference types and add them to the **Interference Types to detect** section.

The following interference types are available:

- BLE Beacon—Bluetooth low energy beacon
- Bluetooth Discovery
- Bluetooth Link
- Canopy
- Continuous Transmitter
- DECT-like Phone—Digital Enhanced Cordless Technology phone
- 802.11 FH—802.11 frequency hopping device
- WiFi Inverted—Device using spectrally inverted Wi-Fi signals
- Jammer
- Microwave Oven
- WiFi Invalid Channel—Device using nonstandard Wi-Fi channels
- TDD Transmitter
- Video Camera
- SuperAG—802.11 SuperAG device
- WiMax Mobile
- WiMax Fixed
- 802.15.4
- Microsoft Device
- SI_FHSS

Step 4 Click **Apply**.

Configuring Interference Reporting for a 2.4-GHz Device (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz cleanair device** {**ble-beacon** | **bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** |	Configures the 2.4-GHz interference devices to report to the device. Run the **no** form of this command to disable the configuration.

	Command or Action	Purpose

	wimax-fixed | wimax-mobile | xbox | zigbee }
	Example:
	`Device(config)# ap dot11 24ghz cleanair device ble-beacon`
	`Device(config)# ap dot11 24ghz cleanair device bt-discovery`
	`Device(config)# ap dot11 24ghz cleanair device bt-link`
	`Device(config)# ap dot11 24ghz cleanair device canopy`
	`Device(config)# ap dot11 24ghz cleanair device cont-tx`
	`Device(config)# ap dot11 24ghz cleanair device dect-like`
	`Device(config)# ap dot11 24ghz cleanair device fh`
	`Device(config)# ap dot11 24ghz cleanair device inv`
	`Device(config)# ap dot11 24ghz cleanair device jammer`
	`Device(config)# ap dot11 24ghz cleanair device mw-oven`
	`Device(config)# ap dot11 24ghz cleanair device nonstd`
	`Device(config)# ap dot11 24ghz cleanair device report`
	`Device(config)# ap dot11 24ghz cleanair device superag`
	`Device(config)# ap dot11 24ghz cleanair device tdd-tx`
	`Device(config)# ap dot11 24ghz cleanair device video`
	`Device(config)# ap dot11 24ghz cleanair device wimax-fixed`
	`Device(config)# ap dot11 24ghz cleanair device wimax-mobile`
	`Device(config)# ap dot11 24ghz cleanair device xbox`
		The following is a list of the keyword descriptions:
		• **ble-beacon**—Bluetooth low energy beacon
		• **bt-discovery**—Bluetooth discovery
		• **bt-link**—Bluetooth link
		• **canopy**—Canopy device
		• **cont-tx**—Continuous transmitter
		• **dect-like**—Digital Enhanced Cordless Communication-like phone
		• **fh**—802.11-frequency hopping device
		• **inv**—Device using spectrally inverted Wi-Fi signals
		• **jammer**—Jammer
		• **mw-oven**—Microwave oven
		• **nonstd**—Device using nonstandard Wi-Fi channels
		• **report**—Interference device reporting
		• **superag**—802.11 SuperAG device
		• **tdd-tx**—TDD transmitter
		• **video**—Video camera
		• **wimax-fixed**—WiMax Fixed
		• **wimax-mobile**—WiMax Mobile
		• **microsoft xbox**—Microsoft Xbox device
		• **zigbee**—802.15.4 device

	Command or Action	Purpose

	`Device(config)# ap dot11 24ghz cleanair device zigbee`
	
	`Device(config)# ap dot11 24ghz cleanair device alarm`	

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling CleanAir for the 5-GHz Band (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**

Step 2 On the **CleanAir** page, click the me**5 GHz Band** > **General** tab.

Step 3 Check the **Enable CleanAir** checkbox.

Step 4 Click **Apply**.

Enabling CleanAir for the 5-GHz Band (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**ap dot11 5ghz cleanair**
	Example:
	`Device(config)#ap dot11 5ghz cleanair`
	
	`Device(config)#no ap dot11 5ghz cleanair`
		Enables the CleanAir feature on a 802.11a network. Run the **no** form of this command to disable CleanAir on the 802.11a network.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Interference Reporting for a 5-GHz Device (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**.

Step 2 Click the **5 GHz Band** tab.

Step 3 Choose the interference types and add them to the **Interference Types to detect** section.

The following interference types are available:

- Canopy
- Continuous Transmitter
- DECT-like Phone—Digital Enhanced Cordless Technology phone
- 802.11 FH—802.11 frequency hopping device
- WiFi Inverted—Device using spectrally inverted Wi-Fi signals
- Jammer
- WiFi Invalid Channel—Device using nonstandard Wi-Fi channels
- SuperAG—802.11 SuperAG device
- TDD Transmitter
- WiMax Mobile
- WiMax Fixed
- Video Camera

Step 4 Click **Apply**.

Configuring Interference Reporting for a 5-GHz Device (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz cleanair device**{**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}	Configures a 5-GHz interference device to report to the device. Run the **no** form of this command to disable interference device reporting.

	Command or Action	Purpose

	Example:
	
	`Device(config)#ap dot11 5ghz cleanair device canopy`
	
	`Device(config)#ap dot11 5ghz cleanair device cont-tx`
	
	`Device(config)#ap dot11 5ghz cleanair device dect-like`
	
	`Device(config)#ap dot11 5ghz cleanair device inv`
	
	`Device(config)#ap dot11 5ghz cleanair device jammer`
	
	`Device(config)#ap dot11 5ghz cleanair device nonstd`
	
	`Device(config)#ap dot11 5ghz cleanair device report`
	
	`Device(config)#ap dot11 5ghz cleanair device superag`
	
	`Device(config)#ap dot11 5ghz cleanair device tdd-tx`
	
	`Device(config)#ap dot11 5ghz cleanair device video`
	
	`Device(config)#ap dot11 5ghz cleanair device wimax-fixed`
	
	`Device(config)#ap dot11 5ghz cleanair device wimax-mobile`
	
	`Device(config)#ap dot11 5ghz cleanair device si_fhss`
	
	`Device(config)#ap dot11 5ghz cleanair device alarm`
		The following is a list of the keyword descriptions:
		• **canopy**—Canopy device
		• **cont-tx**—Continuous transmitter
		• **dect-like**—Digital Enhanced Cordless Communication-like phone
		• **fh**—802.11-frequency hopping device
		• **inv**—Device using spectrally-inverted Wi-Fi signals
		• **jammer**—Jammer
		• **nonstd**—Device using nonstandard Wi-Fi channels
		• **superag**—802.11 SuperAG device
		• **tdd-tx**—TDD transmitter
		• **video**—Video camera
		• **wimax-fixed**—WiMax fixed
		• **wimax-mobile**—WiMax mobile

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Event Driven RRM for a CleanAir Event (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.
The **Radio Resource Management** page is displayed.

Step 2 Click the **DCA** tab.

Step 3 In the **Event Driven RRM** section, check the **EDRRM** check box to run RRM when CleanAir-enabled AP detects a significant level of interference.

Step 4 Configure the **Sensitivity Threshold** level at which RRM has to be invoked from the following options:

- **Low**: Represents a decreased sensitivity to changes in the environment and its value is set at 35.
- **Medium**: Represents medium sensitivity to changes in the environment at its value is set at 50.
- **High**: Represents increased sensitivity to changes in the environment at its value is set at 60.
- **Custom**: If you choose this option, you must specify a custom value in the **Custom Threshold** box.

Step 5 To configure rogue duty cycle, check the **Rogue Contribution** check box and then specify the **Rogue Duty-Cycle** in terms of percentage. The default value of rogue duty cycle is 80 percent.

Note Rogue Contribution is a new component included in ED-RRM functionality. Rogue Contribution allows ED-RRM to trigger based on identified Rogue Channel Utilization, which is completely separate from CleanAir metrics. Rogue Duty Cycle comes from normal off channel RRM metrics, and invokes a channel change based on neighboring rogue interference. Because this comes from RRM metrics and not CleanAir, the timing - assuming normal 180 second off channel intervals - would be within 3 minutes or 180 seconds worst case. It is configured separately from CleanAir ED-RRM and is disabled by default. This allows the AP to become reactive to Wi-Fi interference that is not coming from own network and is measured at each individual AP.

Step 6 Save the configuration.

Configuring EDRRM for a CleanAir Event (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel cleanair-event** **Example:** `Device(config)#ap dot11 24ghz rrm channel cleanair-event`	Enables EDRRM CleanAir event. Run the **no** form of this command to disable EDRRM.

	Command or Action	Purpose
	`Device(config)#no ap dot11 24ghz rrm channel cleanair-event`	
Step 3	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel cleanair-event** [**sensitivity** {**custom** | **high** | **low** | **medium**}] **Example:** `Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures the EDRRM sensitivity of the CleanAir event. The following is a list of the keyword descriptions: • **Custom**—Specifies custom sensitivity to non-Wi–Fi interference as indicated by the AQ value. • **High**—Specifies the most sensitivity to non-Wi–Fi interference as indicated by the AQ value. • **Low**—Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value. • **Medium**—Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

CleanAir Pro Scanning

Feature History for CleanAir Pro Scanning

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 124: Feature History for CleanAir Pro Scanning

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	CleanAir Pro Scanning	The CleanAir Pro Scanning feature monitors and reports the different categories of non-Wi-Fi interference in the 2.4-GHz and 5-GHz bands.
Cisco IOS XE Dublin 17.10.1	CleanAir Support for 6-GHz	The CleanAir is enabled in 6-GHz band radio of AP only if CleanAir is enabled globally in 6-GHz band in the controller and 6-GHz radio of individual AP.

Information About CleanAir Pro Scanning

CleanAir Pro Scanning monitors and provides reports on the different categories of non-Wi-Fi interference, for the 2.4-GHz, 5-GHz, and 6-GHz band. The CleanAir Pro Scanning feature reports the type of interferer, the severity of the interference, and the impacted channels, to the controller, through the Interference Device Reports (IDRs). The air quality (AQ) metric report for each Dynamic Channel Assignment (DCA) channel, contains all the detected non-Wi-Fi interferers and the severity of each interferer.

Note The CleanAir Pro Scanning feature is applicable only for APs with CleanAir Pro-supported radios.

The controller maintains a database of the active interferers reported from each AP. The controller merges interferers across APs if the same interferer is observed across APs. The controller tracks the air quality for each channel and uses the air quality metric report in the channel selection for each AP.

CleanAir Pro Scanning scans channels in slots or bands that are currently enabled on an AP. Channel enablement under DCA is applicable only if you selected the **dca** keyword under the **ap dot11 rrm monitor channel-list** command. The **country** keyword monitors the regulatory channels, and the **all** keyword monitors all channels (everything that the radio can scan, regardless of regulatory constraints).

Interference Device Reports (IDR)

Each AP detects non-Wi-Fi interferers, the duty cycle, Received Signal Strength Indicator (RSSI) in dBm, and a calculated metric known as Severity. These details are sent to the controller through the Interference Device Report (IDR) messages. The IDR event types, such as UP, UPDT, and DOWN, inform the controller about when each interferer was first detected (UP), when the interferer was updated (UPDT),and when it is no longer seen (DOWN). The controller keeps a list of these interferers along with key information, including the channels that are impacted by the interferer on a per-AP basis.

In an AP, interferers are merged with those that are detected on the same channel, same RSSI, and same device signature. This merge occurs on a controller across APs reporting the same type of interferer.

Air Quality Index Reports

The Air Quality (AQ) metric is calculated for each AP, and is the inverse of the cumulative severity metrics. AQ starts at 100 (good) and is decremented by each reported interference source severity metric. For example, if three Bluetooth devices are reported by an AP, each with a severity or two, this will result in the overall cell AQ of 94 (2x3 BT = 6, 100 – 6 = AQ of 94).

Note Cisco IOS XE Cupertino 17.9.1 supports 6-GHz only for spectral analysis on Cisco Catalyst Center. IDR and AQ are not supported for the 6-GHz band in Cisco IOS XE Cupertino 17.9.1.

Enabling CleanAir Pro Scanning (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair** **Example:** `Device(config)# ap dot11 24ghz cleanair`	Configures the CleanAir features for the 2.4-GHz , 5-GHz, or 6-GHz radios.
Step 3	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm air-quality** **Example:** `Device(config)# ap dot11 24ghz cleanair alarm air-quality`	Configures CleanAir alarm for air quality in the 2.4-GHz , 5-GHz, or 6-GHz radios.
Step 4	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm air-quality threshold** *threshold-value* **Example:** `Device(config)# ap dot11 24ghz cleanair alarm air-quality threshold 25`	Configures the air quality threshold value of CleanAir alarm in the 2.4-GHz , 5-GHz, or 6-GHz radios. The valid range is between 1 and 100.
Step 5	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm device cont-tx** **Example:** `Device(config)# ap dot11 24ghz cleanair alarm device cont-tx`	Configures the continuous transmitter as the interference device CleanAir alarm in the 2.4-GHz , 5-GHz, or 6-GHz radios.
Step 6	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm unclassified** **Example:** `Device(config)# ap dot11 24ghz cleanair alarm unclassified`	Configures the air quality alarm on exceeding unclassified category severity.
Step 7	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm unclassified threshold** *threshold-value* **Example:** `Device(config)# ap dot11 24ghz cleanair alarm unclassified threshold 15`	Configures the air quality alarm on exceeding unclassified category severity threshold. The valid range is between 1 and 100.
Step 8	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair device cont-tx** **Example:**	Configure continuous transmitter as the CleanAir interference device type.

	Command or Action	Purpose
	`Device(config)# ap dot11 24ghz cleanair device cont-tx`	

Monitoring CleanAir Pro Statistics (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **CleanAir Statistics**.
The **CleanAir Statistics** window is displayed.

Step 2 Click the **2.4 GHz Band**, **5 GHz Band**, or **6 GHz Band** tab.
The **CleanAir Interference Devices** tab is selected by default. You can monitor and detect the cluster IDs, the interferer type, severity, the affected channels, and so on, for the listed APs.

Step 3 Click the listed devices under the **CleanAir Interference Devices** tab to view the **CleanAir Interference Charts** that displays the **AQ Graph** and the **Interference Power**.

Step 4 Click the **Air Quality** tab to monitor the channel, the average and minimum AQ, number of interferers, the time at which the interference was detected, and the spectrum AP type.

Step 5 Click the **Worst Air Quality Report** tab to view the AQ report, with details of the AP that reported the worst AQ, the radio channel number with the worst-reported air quality, the minimum and the average AQ index, the interference device count, and the spectrum AP type.

Verifying CleanAir Pro Scanning Details

To view the CleanAir Air Quality (AQ) data, run the following command:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} cleanair air-quality summary
```

To view the CleanAir Air Quality (AQ) worst data, run the following command:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} cleanair air-quality worst
```

To view the CleanAir device cluster information, run the following command:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} cleanair device cluster cluster-id
```

To view the CleanAir interferers of a device type, run the following command:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} cleanair device type
```

To view the CleanAir configuration for a specific AP, run the following commands:

```
Device# show ap name ap-name dot11 {24ghz | 5ghz | 6ghz} cleanair air-quality
Device# show ap name ap-name dot11 {24ghz | 5ghz | 6ghz} cleanair device
```

To view the continuous transmitter as the CleanAir interference device type, run the following command:

```
Device# show ap dot11 6ghz cleanair device type cont-tx
```

Verifying CleanAir Parameters

You can verify CleanAir parameters using the following commands:

Table 125: Commands for verifying CleanAir

Command Name	Description
show ap dot11 24ghz cleanair device type all	Displays all the CleanAir interferers for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type ble-beacon	Displays all the Bluetooth BLE beacons for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type bt-discovery	Displays CleanAir interferers of type BT Discovery for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type bt-link	Displays CleanAir interferers of type BT Link for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type canopy	Displays CleanAir interferers of type Canopy for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type cont-tx	Displays CleanAir interferers of type Continuous transmitter for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type dect-like	Displays CleanAir interferers of type DECT Like for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type fh	Displays CleanAir interferers of type 802.11FH for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type inv	Displays CleanAir interferers of type Wi-Fi Inverted for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type jammer	Displays CleanAir interferers of type Jammer for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type mw-oven	Displays CleanAir interferers of type MW Oven for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type nonstd	Displays CleanAir interferers of type Wi-Fi inverted channel for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type superag	Displays CleanAir interferers of type SuperAG for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type tdd-tx	Displays CleanAir interferers of type TDD Transmit for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type video	Displays CleanAir interferers of type Video Camera for the 2.4-GHz band.

Command Name	Description
show ap dot11 24ghz cleanair device type wimax-fixed	Displays CleanAir interferers of type WiMax Fixed for the 2.4-GHz band.

Monitoring Interference Devices

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. Some devices conserve power by limiting the transmit time until actually needed, which results in the spectrum sensor to stop detecting the device temporarily. This device is then correctly marked as down. Such a device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific device are reported, the cluster ID is kept alive for an extended period of time to prevent possible device-detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device-detection history is preserved.

For example, some Bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs for longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Note The following is a prerequisite for monitoring the interference devices:

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Configuration Examples for CleanAir

This example shows how to enable CleanAir on the 2.4-GHz band and an access point operating in the channel:

```
Device#configure terminal
Device(config)#ap dot11 24ghz cleanair
Device(config)#exit
Device#ap name TAP1 dot11 24ghz cleanair
Device#end
```

This example shows how to enable an EDRRM CleanAir event in the 2.4-GHz band and configure high sensitivity to non-Wi–Fi interference:

```
Device#configure terminal
Device(config)#ap dot11 24ghz rrm channel cleanair-event
Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Device(config)#end
```

This example shows how to enable an access point in the monitor mode:

```
Device#ap name <ap-name> mode monitor
```

CleanAir FAQs

Q. Multiple access points detect the same interference device. However, the device shows them as separate clusters or different suspected devices clustered together. Why does this happen?

A. Access points must be RF neighbors for the device to consider merging the devices that are detected by these access points. An access point takes time to establish neighbor relationships. A few minutes after the device reboots or after there is a change in the RF group, and similar events, clustering will not be very accurate.

Q. How do I view neighbor access points?

A. To view neighbor access points, use the **show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**} command.

This example shows how to display the neighbor access points:

```
Device#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                          :  -12 dBm on   1 (10.10.0.5)
  AP 0C85.25AB.CCA0 slot 0                          :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25C7.B7A0 slot 0                          :  -26 dBm on  11 (10.10.0.5)
  AP 0C85.25DE.2C10 slot 0                          :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25DE.C8E0 slot 0                          :  -14 dBm on  11 (10.10.0.5)
  AP 0C85.25DF.3280 slot 0                          :  -31 dBm on   6 (10.10.0.5)
  AP 0CD9.96BA.5600 slot 0                          :  -44 dBm on   6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0                          :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. What are the AP debug commands available for CleanAir?

A. The AP debug commands for CleanAir are:

- **debug cleanair** {**bringup** | **event** | **logdebug** | **low** | **major** | **nsi** | **offchan**}
- **debug rrm** {**neighbor** | **off-channel** | **reports**}

CHAPTER 154

Bluetooth Low Energy

- Information About Bluetooth Low Energy, on page 1653
- Enabling Bluetooth Low Energy Beacon (GUI), on page 1654
- Enabling Bluetooth Low Energy Beacon, on page 1654

Information About Bluetooth Low Energy

Note This feature is not related to the Indoor IoT Services feature set that is part of Cisco Spaces.

This feature describes how Access Points and Catalyst 9800 can detect BLE devices as wireless interferers using Clean Air - not the BLE radio that is available on some Access Point models. This feature is not meant to be used for BLE-based asset tracking, environmental monitoring, or tag management use cases, which are powered using Cisco Spaces.

For full feature functionality of how BLE-related use cases are delivered in the Cisco solution, refer to Cisco Spaces configuration guides for Indoor IoT services.

Bluetooth low energy (BLE) is a wireless personal area network technology aimed at enhancing location services for mobile devices. The small Bluetooth tag devices placed at strategic locations transmit universally unique identifiers (UUIDs) and, Major and Minor fields as their identity. These details are picked up by Bluetooth-enabled smartphones and devices. The location information of these devices are sent to the corresponding back-end server. Relevant advertisements and other important information are then pushed to the devices using this location-specific information.

By treating a tag device as an interferer and using the existing system capabilities, such as interference location, the tag device can be located on a map display in a wireless LAN deployment and its movement monitored. Besides this, information on missing tags can also be obtained. This feature can determine rogue and malicious tags using the unique identifier associated with each tag (or family of tags) against a predetermined allowed list from a customer. Using the management function, alerts can be displayed or emailed based on rogue tags, missing tags, or moved tags.

Limitations of BLE Feature

- The wireless infrastructure must support Cisco CleanAir.
- Supports a maximum of only 250 unique BLE beacons (cluster entries) and 1000 device entries.

- Cisco CleanAir feature is only supported on Cisco Aironet 3700 Series Access Points with Hyperlocation module RM3010. The BLE feature on Wave 2 and Wi-Fi 6 APs works in a different manner (through cloud beacon center) and is not covered by this feature.

Areas of Use

Since the BLE feature provides granular location details of devices (smart phones or bluetooth-enabled devices) that helps push context-sensitive advertising and other information to users. Possible areas of application include retail stores, museums, zoo, healthcare, fitness, security, advertising, and so on.

Enabling Bluetooth Low Energy Beacon (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir** > **2.4 GHz Band** > **General**.

Step 2 Check the **Enable CleanAir** check box.

Step 3 From the **Available Interference Types** list, select and move **BLE Beacon** to the **Interference Types to Detect** list.

Step 4 Click **Apply**.

Enabling Bluetooth Low Energy Beacon

Bluetooth low energy (BLE) detection is enabled by default. Use the procedure given below to enable BLE when it is disabled.

Before you begin

- The wireless infrastructure must support Cisco CleanAir.
- Cisco CleanAir configuration and show commands are available only in Mobility Controller (MC) mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **ap dot11 24ghz cleanair device** [**ble-beacon**] **Example:** `Controller(config)# ap dot11 24ghz cleanair device ble-beacon`	Enables the BLE feature on the 802.11b network. Use the **no** form of the command to disable BLE feature on the 802.11b network.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Controller(config)# exit`	Returns to privileged EXEC mode.

Step 4	**show ap dot11 24ghz cleanair config**
	Example:
	`Controller# show ap dot11 24ghz cleanair config`
	
	`Interference Device Settings:`
	`Interference Device Reporting..... : Enabled`
	`Bluetooth Link..... : Enabled`
	
	`Microwave Oven..... : Enabled`
	
	`BLE Beacon..... : Enabled`
		(Optional) Displays the BLE beacon configuration.

Step 5	**show ap dot11 24ghz cleanair device type ble-beacon**
	Example:
	`Controller# show ap dot11 24ghz cleanair device type ble-beacon`
	
	`DC = Duty Cycle (%)`
	`ISI = Interference Severity Index (1-Low Interference, 100-High Interference)`
	`RSSI = Received Signal Strength Index (dBm)`
	`DevID = Device ID`
	
	`No ClusterID DevID Type AP Name ISI RSSI DC Channel`
	`1 2c:92:80:00:00:22 0xa001 BLE Beacon 5508_3_AP3600_f839 -- -74 0 unknown`
		(Optional) Displays the BLE beacon device-type information.

CHAPTER 155

Persistent Device Avoidance

- Information about Cisco Persistent Device Avoidance, on page 1657
- Configuring Persistent Device Avoidance (GUI), on page 1658
- Configuring Persistent Device Avoidance (CLI), on page 1658
- Verifying Persistent Device Avoidance, on page 1658

Information about Cisco Persistent Device Avoidance

The Cisco CleanAir Persistent device avoidance (PDA) feature is a part of spectrum management. Some interference devices, such as, outdoor bridges and microwave ovens, transmit signals only when required. These devices can cause significant interference to the local WLAN, because short-duration and periodic operations remain largely undetected by normal RF management metrics. With Cisco CleanAir (CleanAir), the RRM dynamic channel allocation (DCA) algorithm can detect, measure, register, and remember the impact, and adjust the RRM DCA algorithm. The PDA process minimizes the use of channels affected by persistent devices in the channel plan, local to the interference source. CleanAir detects and stores persistent device information in the controller. This information is used to mitigate the interfering channels.

Persistent Devices Detection - CleanAir-capable monitor mode APs collect information about persistent devices on all the configured channels and store the information in the controller. Local or bridge mode APs detect interference devices only on the serving channels.

The PDA feature works seamlessly on all platforms. All the AP models that are capable of CleanAir and Spectrum Intelligence support the PDA feature.

The supported platforms are:

- Cisco Aironet 1852 Access Points
- Cisco Aironet 1832 Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9115 Series Access Points

- Cisco Catalyst 9117 Series Access Points
- Cisco Catalyst 9120AX Series Access Points
- Cisco Catalyst 9124AX Series Access Points
- Cisco Catalyst 9130AX Access Points

Configuring Persistent Device Avoidance (GUI)

Procedure

Step 1 Choose **Configurations** > **Radio Configurations** > **RRM**

Step 2 Click the **5 GHz Band** tab or the **2.4 GHz Band**, and click the **DCA** tab.

Step 3 In the **DCA** window, under the **Dynamic Channel Assignment Algorithm** section, check the **Avoid Persistent Non-WiFi Interference** check box to enable the device to ignore persistent non-WiFi interference.

Step 4 Click **Apply**.

Configuring Persistent Device Avoidance (CLI)

You can enable and disable the PDA feature and PDA propagation configuration mode through the RRM Manager.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**[no] ap dot11 {24ghz | 5ghz} rrm channel device** **Example:** `Device# [no] ap dot11 24ghz rrm channel device`	Configures persistent non-WiFi device avoidance in the 802.11a or 802.11b channel assignment. Use the **no** form of this command to negate the command or to set its defaults.

Verifying Persistent Device Avoidance

To verify the current state of **Device Aware** detail of the channel, use the following command:

```
Device#show ap dot11 24ghz channel
Leader Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
```

```
  Channel Update Interval                    : 600 seconds
  Anchor time (Hour of the day)              : 0
  Channel Update Contribution
    Noise                                    : Enable
    Interference                             : Enable
    Load                                     : Disable
    Device Aware                         :   Enable
  CleanAir Event-driven RRM option           : Disabled
  Channel Assignment Leader                  : cisco-vwlc (9.9.39.73)
  Last Run                                   : 166 seconds ago

  DCA Sensitivity Level                      : MEDIUM : 10 dB
  DCA Minimum Energy Limit                   : -95 dBm
  Channel Energy Levels
    Minimum                                  : -82 dBm
    Average                                  : -82 dBm
    Maximum                                  : -82 dBm
  Channel Dwell Times
    Minimum                                  : 8 days 0 hour 43 minutes 13 seconds
    Average                                  : 8 days 0 hour 43 minutes 13 seconds
    Maximum                                  : 8 days 0 hour 43 minutes 13 seconds
  802.11b 2.4 GHz Auto-RF Channel List
    Allowed Channel List                     : 1,6,11
    Unused Channel List                      : 2,3,4,5,7,8,9,10
```

```
Device#show ap dot11 24ghz cleanair device type all
DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
PD    = Persistent Device

ClusterID          Mac Address        DevID  Type           PD   AP Name
        Version  ISI  RSSI  DC   Channel              Last Update Time
-------------------------------------------------------------------------------------------------
9800.0000.0004     3400.0200.0001     0x0001 Jammer         No   RRM-TSIM-1
        CA       100  -67   100  1,2                  12/16/2020 18:32:42 UTC
9800.0000.0005     3400.0200.0004     0x0004 Xbox           No   RRM-TSIM-1
        CA       45   -73   45   1                    12/16/2020 18:32:42 UTC
9800.0000.0006     3400.0200.0006     0x0006 TDD Transmit   No   RRM-TSIM-1
        CA       10   -75   10   1,2                  12/16/2020 18:32:42 UTC
9800.0000.0006     3400.0200.0007     0x0007 Continuous TX  No   RRM-TSIM-1
        CA       30   -77   30   1,2                  12/16/2020 18:32:42 UTC
9800.0000.0007     3400.0200.0009     0x0009 802.15.4       No   RRM-TSIM-1
        CA       10   -95   10   1,2                  12/16/2020 18:32:42 UTC
```

```
Device# show ap dot11 5ghz cleanair device type all
DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
PD    = Persistent Device

ClusterID          Mac Address        DevID  Type           PD   AP Name
        Version  ISI  RSSI  DC   Channel              Last Update Time
-------------------------------------------------------------------------------------------------
9800.0000.0000     3400.0201.0002     0x0002 WiFi Inverted  No   RRM-TSIM-1
        CA       45   -63   45   40                   12/16/2020 18:32:42 UTC
9800.0000.0001     3400.0201.0004     0x0004 TDD Transmit   No   RRM-TSIM-1
        CA       10   -76   10   40                   12/16/2020 18:32:42 UTC
9800.0000.0001     3400.0201.0005     0x0005 Continuous TX  No   RRM-TSIM-1
        CA       30   -77   30   40                   12/16/2020 18:32:42 UTC
9800.0000.0002     3400.0201.0007     0x0007 BT Link        No   RRM-TSIM-1
        CA       10   -88   10   40                   12/16/2020 18:32:42 UTC
```

To verify all the reported interferers along with the class type, use the following command:

```
Device# show ap dot11 24ghz cleanair device type wimax-mobile
DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

ClusterID          Mac Address        DevID  Type          AP Name                     ISI
  RSSI  DC   Channel
------------------------------------------------------------------------------------------------------
1900.0000.0006     xxxx.xxxx.xxx1     0xc001 WiMax Mobile  Cisco-AP                     4
   -88   1
1900.0000.0007     xxxx.xxxx.xxx2     0xc002 WiMax Mobile  Cisco-AP                     4
   -88   1
```

To verify the persistent device information under Auto-RF, use the following command:

```
Device#show ap auto-rf dot11 24ghz
Number of Slots            : 2
AP Name                    : VANC-AP
MAC Address                : d4c9.3ce5.c760
Slot ID                    : 0
Radio Type                 : 802.11n - 2.4 GHz
….….….….
Noise Information
……...
Persistent Interference Devices
Class Type                 Channel  DC (%%)  RSSI (dBm)  Last Update Time
-------------------------  -------  ------   ---------   ----------------
MW Oven                     11      NA        -71        08/22/2019 12:03:18 UTC
MW Oven                     11      NA        -24        08/22/2019 12:03:19 UTC
MW Oven                     11      NA        -17        08/22/2019 12:03:16 UTC
MW Oven                     11      NA        -22        08/22/2019 12:03:19 UTC
```

To verify the persistent device information under Auto-RF for specific Cisco APs, use the following command:

```
Device#show ap name ap_name auto-rf dot11 24ghz

Number of Slots            : 2
AP Name                    : VANC-AP
MAC Address                : d4c9.3ce5.c760
Slot ID                    : 0
Radio Type                 : 802.11n - 2.4 GHz
….….….….
Noise Information
……...
Persistent Interference Devices
Class Type                 Channel  DC (%%)  RSSI (dBm)  Last Update Time
-------------------------  -------  ------   ---------   ----------------
MW Oven                     11      NA        -71        08/22/2019 12:03:18 UTC
MW Oven                     11      NA        -24        08/22/2019 12:03:19 UTC
MW Oven                     11      NA        -17        08/22/2019 12:03:16 UTC
MW Oven                     11      NA        -22        08/22/2019 12:03:19 UTC
```

CHAPTER 156

Spectrum Intelligence

- Spectrum Intelligence, on page 1661
- Configuring Spectrum Intelligence, on page 1662
- Verifying Spectrum Intelligence Information, on page 1662
- Debugging Spectrum Intelligence on Supported APs (CLI), on page 1663

Spectrum Intelligence

The Spectrum Intelligence feature scans for non-Wi-Fi radio interference on 2.4-GHz and 5-GHz bands. Spectrum intelligence provides basic functions to detect interferences of three types, namely microwave, continuous wave (like video bridge and baby monitor), wi-fi and frequency hopping (Bluetooth and frequency-hopping spread spectrum (FHSS) cordless phone).

The following Cisco access points (APs) support Spectrum Intelligence feature:

- Cisco Catalyst 9105 Series Wi-Fi 6 APs
- Cisco Catalyst 9115 Series Wi-Fi 6 APs
- Cisco Aironet 1852E/I APs
- Cisco Aironet 1832I APs
- Cisco Aironet 1815W/T/I/M APs
- Cisco Aironet 1810W/T APs
- Cisco Aironet 1800I/S APs
- Cisco Aironet 1542D/I APs

Note You must enable Spectrum Intelligence feature on the Cisco Aironet 1832 and 1852 series APs to get radio details, such as noise, air-quality, interference, and radio utilization on the Cisco Catalyst Center Assurance AP health.

Restrictions

- SI APs only report a single interference type in Local mode.

- SI does not support high availability for air quality or interference reports. High Availability is not supported because interference report/device reported will not be copied to standby after switchover. We expect AP to send it again, if at all interferer is still there.
- Spectrum Intelligence detects only three types of devices:
  - Microwave
  - Continuous wave—(video recorder, baby monitor)
  - SI-FHSS—(Bluetooth, Frequency hopping Digital European Cordless Telecommunications (DECT) phones)

Configuring Spectrum Intelligence

Follow the procedure given below to configure spectrum intelligence:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **SI** **Example:** `Device(config)# ap dot11 24ghz SI`	Configures the 2.4-GHz or 5-GHz Spectrum Intelligence feature on the 802.11a or 802.11b network. Add **no** form of the command to disable SI on the 802.11a or 802.11b network.

Verifying Spectrum Intelligence Information

Use the following commands to verify spectrum intelligence information:

To display the SI information for a 2.4-GHz or 5-GHz band, use the following command:

```
Device# show ap dot11 24ghz SI config

SI Solution..................................... : Enabled
Interference Device Settings:
        SI_FHSS............................... : Enabled
    Interference Device Types Triggering Alarms:
        SI_FHSS............................... : Disabled
```

```
Device# show ap dot11 5ghz SI device type
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
PD    = Persistent Device

Mac Address        DevID  Type          PD   AP Name                          RSSI  Channel
             Last Update Time
```

```
3400.0401.0006     0x0006 BT Discovery   No   RRM-TSIM-3                        -88   40
                12/16/2020 18:11:28 UTC
```

To display SI interferers of type Continuous transmitter for a 2.4-GHz band, use the following command:

```
Device# show ap dot11 24ghz SI device type cont_tx
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

Mac Address        DevID  Type          AP Name                              RSSI  Channel
-------------------------------------------------------------------------------------------
xxxx.xxxx.xxxx     0xf001 Continuous TX Cisco-AP                          -47
```

To display 802.11a interference devices information for the given AP for 5-GHz, use the following command:

```
Device# show ap dot11 5ghz SI device type ap

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
AP type = CA, clean air, SI spectrum intelligence

No  ClusterID/BSSID    DevID  Type    AP Type AP Name                ISI  RSSI  DC   Channel
--- ------------------ ------ ------- ------  ---------------------- ---- ----- ---- ----------
```

To display SI interferers of type Continuous transmitter for a 5-GHz band, use the following command:

```
Device# show ap dot11 5ghz SI device type cont_tx
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

Mac Address        DevID  Type          AP Name                              RSSI  Channel
-------------------------------------------------------------------------------------------
xxxx.xxxx.xxx1     0xf001 Continuous TX Cisco-AP                             -88

xxxx.xxxx.xxx2     0xf002 Continuous TX Cisco-AP                             -88
```

To display all Cisco CleanAir interferers for a 2.4-GHz band, use the following command:

```
Device# show ap dot11 24ghz cleanair device type all
```

Debugging Spectrum Intelligence on Supported APs (CLI)

You need to enter these commands in the AP console. For information about APs that support this feature see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.

Procedure

- Generate major Spectrum Intelligence logs for an AP by entering this command:
  debug cleanair major

- Verify the Spectrum Intelligence scan schedule of 5 seconds on an AP by entering this command:
  debug cleanair event

- Generate logs at 10-minute interval, when interference is not detected or reported by the AP, by entering this command:

  debug cleanair raw 10

  This command creates three files under **/tmp** directory from dev shell.

  - spectrum.fft
  - spectrum.dbg
  - spectrum.int

- View the Spectrum Intelligence detected interfering devices by entering this command:

  show cleanair interferers

- View the Spectrum Intelligence configuration status by entering this command:

  show cleanair status

CHAPTER 157

Spectrum Analysis

- Information About Spectrum Analysis, on page 1665
- Live Spectrum Analysis, on page 1666
- Performing AP Spectrum Analysis (GUI), on page 1666
- Configuring Spectrum Analysis, on page 1667
- Verifying Spectrum Analysis, on page 1667

Information About Spectrum Analysis

Cisco Catalyst Center receives a spectrogram stream from access points and visualizes spectrum analysis as a real-time spectrogram view. Network administrators receive RF violation issues from end users or radio frequency issue from the Catalyst Center. To analyze a violation, you should select the corresponding AP and analyze the spectrogram stream.

Based on whether a setting is global or is meant for a specific channel, every AP uses a specific channel to communicate with clients.

When a lot of clients join on the same AP, there is a high possibility of frames getting dropped off. When there is an issue of clients dropping quickly, or not getting onboarded, you should perform the spectrum analysis to check if the channels are clogged.

You can enable spectrum analysis on every AP listed in the web UI and view the graphs based on the corresponding AP. When enabled, the APs send spectrum data to Catalyst Center which then aggregates it into 3 distinct charts.

You can view the following charts while performing a spectrum analysis:

- Persistence Charts: Plot the amplitude-to-power ratio of each signal at each channel for a period of five minutes. The chart is color coded with blue color representing one signal and red representing many signals. This chart also plots the opacity that represents the age of the signal data within the five minute interval, with older data being more transparent.
- Waterfall Charts: Plot all the signals that are analyzed in the channel for a period of five minutes with intensity on X axis, and with time represented in the Y axis. The chart is color coded, with blue color representing a low value and red representing a high value.
- Interference and Duty Charts: Plot the severity of detected interference for each channel band, and list the interference type. Interference is plotted as a circle, where the center represents the severity, and the radius represents the section of the channel band that is affected. The impact of the interference is measured

as severity, with values ranging from 0 to 100. The interference type is determined from RF signature identified by Cisco CleanAir technology of the interference.

Live Spectrum Analysis

You can perform a live spectrum analysis of the AP radios, and monitor the spectrum of frequencies generated by the radios of the corresponding AP using the web UI. The live spectrum capture uses radio 2 if it is available. Otherwise, both radio 0 and radio 1 are used. When you enable live spectrum analysis on radio 2, Cisco Catalyst Center displays a consolidated view of the interference in both the 2.4 Ghz and 5 Ghz range. However; if the feature is enabled on radio 0 or radio 1, you can only view the part of the spectrum that the radios are associated with. You can select a radio in the web UI and view a live spectrum associated with this radio, for 10 minutes, and later extend the duration based on your requirement.

Performing AP Spectrum Analysis (GUI)

Before you begin

Use the Cisco Catalyst Center Discovery functionality to locate an AP to perform a spectrum analysis. .

Procedure

Step 1 Choose **Provision** > **Inventory**.

The **Inventory** window is displayed.

Step 2 Click **AP Name** .

The **360 degree Device** window is displayed.

Step 3 Click **Intelligent Capture** .

Step 4 Click **Spectrum Analysis** to view the graphs.

Step 5 From the **Radio** drop-down list, choose a radio.

Step 6 Click **Start Spectrum Analysis** .

The graphs are displayed on the web UI for you to analyze.

To stop the analysis, click **Stop Spectrum Analysis**.

Configuring Spectrum Analysis

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**icap subscription ap rf spectrum enable** **Example:** `Device# icap subscription ap rf spectrum enable`	Configures spectrum analysis on the AP.
Step 3	**icap subscription ap rf spectrum slot***number* **Example:** `Device# icap subscription ap rf spectrum slot 0`	Selects a radio slot to enable spectrum analysis.

Verifying Spectrum Analysis

The following is a sample output of the **show ap icap subscription name** command that verifies spectrum analysis on a selected AP:

```
Device#show ap icap subscription name
Subscription list
-----------------
Full Pkt Capture : Disabled
Partial Pkt Capture : Enabled
Anomaly Event : Enabled
Debug : Disabled
Stats : Disabled
Ap Operational Data : Disabled
Sensor Message : Enabled
RRM Operational Data : Disabled
Client Events : Disabled
aWIPS Forensic Pkts: Disabled

MAC and Filters subscription list
---------------------------------
Full-packet-trace: None
Partial-packet-trace: None
Filters: None
Anomaly Detection: None

Client Stats
------------
None

RF Spectrum
```

```
-----------
Radio Slot(s): 1
```

PART XIII

Mesh Access Points

- Mesh Access Points, on page 1671
- Redundant Root Access Point (RAP) Ethernet Daisy Chaining, on page 1747

CHAPTER 158

Mesh Access Points

- Introduction to the Mesh Network, on page 1673
- Restrictions for Mesh Access Points, on page 1674
- MAC Authorization, on page 1676
- Preshared Key Provisioning, on page 1676
- EAP Authentication, on page 1676
- Bridge Group Names, on page 1677
- Background Scanning, on page 1678
- Information About Background Scanning and MAP Fast Ancestor Find Mode , on page 1678
- Mesh Backhaul at 2.4 GHz and 5 GHz , on page 1679
- Information About Mesh Backhaul, on page 1679
- Information About Mesh Serial Backhaul, on page 1680
- Information About Mesh Backhaul RRM, on page 1681
- Dynamic Frequency Selection, on page 1682
- Country Codes, on page 1682
- Intrusion Detection System, on page 1683
- Mesh Interoperability Between Controllers, on page 1683
- Information About DHCP and NAT Functionality on Root AP (RAP), on page 1683
- Mesh Convergence, on page 1684
- Ethernet Bridging, on page 1684
- Multicast Over Mesh Ethernet Bridging Network, on page 1685
- Radio Resource Management on Mesh, on page 1686
- Air Time Fairness on Mesh, on page 1686
- Spectrum Intelligence for Mesh, on page 1687
- Indoor Mesh Interoperability with Outdoor Mesh, on page 1687
- Workgroup Bridge, on page 1687
- Link Test, on page 1688
- Mesh Daisy Chaining, on page 1688
- Mesh Leaf Node, on page 1689
- Flex+Bridge Mode, on page 1689
- Backhaul Client Access, on page 1689
- Mesh CAC, on page 1689
- Prerequisites for Mesh Ethernet Daisy Chaining, on page 1690
- Restrictions for Mesh Ethernet Daisy Chaining, on page 1690

- Speeding up Mesh Network Recovery Through Fast Detection of Uplink Gateway Reachability Failure, on page 1691
- Fast Teardown for a Mesh Deployment, on page 1691
- Configuring MAC Authorization (GUI), on page 1691
- Configuring MAC Authorization (CLI), on page 1692
- Configuring MAP Authorization - EAP (GUI), on page 1693
- Configuring MAP Authorization (CLI), on page 1694
- Configuring PSK Provisioning (CLI), on page 1695
- Configuring a Bridge Group Name (GUI), on page 1696
- Configuring a Bridge Group Name (CLI), on page 1696
- Configuring Background Scanning (GUI), on page 1697
- Configuring Background Scanning, on page 1697
- Configuring AP Fast Ancestor Find Mode (GUI), on page 1698
- Configuring Background Scanning and MAP Fast Ancestor Find Mode (CLI), on page 1698
- Configuring Backhaul Client Access (GUI), on page 1699
- Configuring Backhaul Client Access (CLI), on page 1699
- Configuring Dot11ax Rates on Mesh Backhaul Per Access Point (GUI), on page 1700
- Configuring Dot11ax Rates on Mesh Backhaul in Mesh Profile (GUI), on page 1700
- Configuring Wireless Backhaul Data Rate (CLI), on page 1701
- Configuring Data Rate Per AP (CLI), on page 1702
- Configuring Data Rate Using Mesh Profile (CLI), on page 1702
- Configuring Mesh Backhaul (CLI), on page 1703
- Configuring Dynamic Frequency Selection (CLI), on page 1703
- Configuring the Intrusion Detection System (CLI), on page 1704
- Configuring Ethernet Bridging (GUI), on page 1704
- Configuring Ethernet Bridging (CLI), on page 1705
- Configuring Multicast Modes over Mesh, on page 1706
- Configuring RRM on Mesh Backhaul (CLI), on page 1707
- Configuring RRM Channel Assignment for Root Access Points Globally, on page 1708
- Configuring RRM Channel Assignment for an Access Point, on page 1709
- Selecting a Preferred Parent (GUI), on page 1709
- Selecting a Preferred Parent (CLI), on page 1709
- Changing the Role of an AP (GUI), on page 1711
- Changing the Role of an AP (CLI), on page 1711
- Configuring the Mesh Leaf Node (CLI), on page 1711
- Configuring the Mesh Leaf Node (GUI), on page 1712
- Configuring Subset Channel Synchronization , on page 1712
- Provisioning LSC for Bridge-Mode and Mesh APs (GUI), on page 1713
- Provisioning LSC for Bridge-Mode and Mesh APs, on page 1713
- Specifying the Backhaul Slot for the Root AP (GUI), on page 1714
- Specifying the Backhaul Slot for the Root AP (CLI), on page 1714
- Using a Link Test on Mesh Backhaul (GUI), on page 1715
- Using a Link Test on Mesh Backhaul, on page 1715
- Configuring Battery State for Mesh AP (GUI), on page 1716
- Configuring Battery State for Mesh AP, on page 1716
- Configuring Mesh Convergence (CLI), on page 1717

• Configuring DHCP Server on Root Access Point (RAP), on page 1717
• Configuring Mesh Ethernet Daisy Chaining (CLI), on page 1718
• Enabling Mesh Ethernet Daisy Chaining, on page 1718
• Configuring Mesh CAC (CLI), on page 1719
• Configuring ATF on Mesh (GUI), on page 1719
• Configuring ATF on Mesh, on page 1720
• Create an ATF Policy for a MAP, on page 1720
• Creating an ATF Policy (GUI), on page 1721
• Adding an ATF to a Policy Profile (GUI), on page 1721
• Enabling ATF Mode in an RF Profile (GUI), on page 1721
• Enabling Wireless Mesh Profile, on page 1722
• Enabling Serial Backhaul in Radio Profile (GUI), on page 1722
• Enabling Mesh Configurations in Radio Profile (CLI), on page 1723
• Enabling Serial Backhaul (CLI), on page 1724
• Associating Wireless Mesh to an AP Profile (CLI), on page 1725
• Configuring Fast Teardown for a Mesh AP Profile (GUI) , on page 1725
• Configuring Fast Teardown for a Mesh AP Profile (CLI), on page 1726
• Flex Resilient with Flex and Bridge Mode Access Points, on page 1727
• Verifying ATF Configuration on Mesh, on page 1733
• Verifying Mesh Ethernet Daisy Chaining, on page 1734
• Verifying Mesh Convergence, on page 1734
• Verifying DHCP Server for Root AP Configuration, on page 1735
• Verifying Mesh Backhaul, on page 1735
• Verifying Mesh Configuration, on page 1736
• Verifying Dot11ax Rates on Mesh Backhaul, on page 1744
• Verifying Mesh Serial Backhaul, on page 1744
• Verifying the RRM DCA Status, on page 1745
• Verifying Fast Teardown with Default Mesh Profile, on page 1745
• Verifying Background Scanning and MAP Fast Ancestor Find, on page 1746

Introduction to the Mesh Network

Mesh networking employs Cisco Aironet outdoor mesh access points and indoor mesh access points along with Cisco Wireless Controller and Cisco Prime Infrastructure to provide scalability, central management, and mobility between indoor and outdoor deployments. Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network.

End-to-end security within the mesh network is supported by employing Advanced Encryption Standard (AES) encryption between wireless mesh access points and Wi-Fi Protected Access 2 (WPA2) clients. For connections to a mesh access point (MAP) wireless client, such as MAP-to-MAP and MAP-to-root access point, WPA2 is applicable.

The wireless mesh terminates on two points on the wired network. The first location is where the root access point (RAP) is attached to the wired network, and where all bridged traffic connects to the wired network. The second location is where the CAPWAP controller connect to the wired network; this location is where the WLAN client traffic from the mesh network is connected to the wired network. The WLAN client traffic from CAPWAP is tunneled to Layer 2. Matching WLANs should terminate on the same switch VLAN on

which the wireless controllers are co-located. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the wireless controller is connected.

In the new configuration model, the controller has a default mesh profile. This profile is mapped to the default AP-join profile, which is in turn is mapped to the default site tag. If you are creating a named mesh profile, ensure that these mappings are put in place, and the corresponding AP is added to the corresponding site-tag.

Important The following are the mesh supported scenarios in IRCM from Cisco IOS XE Amsterdam 17.3 release up to Cisco IOS XE Cupertino 17.9 release, for the Cisco Wave 1 APs that are not supported:

- Cisco Wave 1 APs are not supported in the releases post Cisco IOS XE Amsterdam 17.3. This includes mesh support as well. Therefore, it is not possible for a Cisco Wave 1 AP to join a Cisco Catalyst 9800 Series Wireless Controller (controller) with Cisco IOS XE Amsterdam 17.4 and later versions. We recommend the following deployment mode for Cisco Wave 1 APs.
- In the case of Cisco mesh deployments, the following are the deployment limitations to be aware of, when the system is deployed:
  - MAP roaming is not allowed between Cisco Catalyst 9800 Series Wireless Controllers, if the controllers run different Cisco IOS XE versions (running on versions Cisco IOS XE Amsterdam 17.3 or Cisco IOS XE Cupertino 17.9) for any of the Cisco Wave 1 APs and Cisco Wave 2 APs.
  - You cannot have Cisco Wave 1 APs and Cisco Catalyst 9124 Series APs in the same mesh tree, in the releases post Cisco IOS XE Amsterdam 17.3.x. This can be achieved in 17.3.x, beginning from the 17.3.6 (upcoming) release.
  - The whole mesh tree containing Cisco Wave 1 APs must be joined to the 17.3 controller, by running the **strict-bgn** and **mac filtering** commands.

Note The limitations mentioned above are not valid for the Cisco Industrial Wireless 3702 Se which are supported until the Cisco IOS XE Cupertino 17.9 release.

Cisco Catalyst 9130AXE Access Points support Serial Backhaul with omni antenna using dart connectors.Cisco Catalyst 9130AXI APs supports Serial Backhaul, as the second 5-GHz radio is for macro and micro cell (the transmission power of the second 5-GHz radio cannot be changed).

Restrictions for Mesh Access Points

The Mesh feature is supported only on the following AP platforms:

- Outdoor APs
  - Cisco Industrial Wireless 3702 Access Points (supported from Cisco IOS XE Gibraltar 16.11.1b).
  - Cisco Aironet 1542 Access Points
  - Cisco Aironet 1562 Access Points
  - Cisco Aironet 1572 Access Points

- Cisco Catalyst IW6300 Heavy Duty Access Points
- Cisco 6300 Series Embedded Services Access Points
- Cisco Catalyst 9124AX Series Outdoor Access Points
- Cisco Catalyst IW9167 Series Heavy Duty Access Points

- Indoor APs
  - Cisco Aironet 1815i Access Points
  - Cisco Aironet 1815m Access Points
  - Cisco Aironet 1815w Access Points
  - Cisco Aironet 1832i Access Points
  - Cisco Aironet 1852i Access Points
  - Cisco Aironet 1852e Access Points
  - Cisco Aironet 2802i Access Points
  - Cisco Aironet 2802e Access Points
  - Cisco Aironet 3802i Access Points
  - Cisco Aironet 3802e Access Points
  - Cisco Aironet 3802p Access Points
  - Cisco Aironet 4800 Access Points
  - Cisco Catalyst 9130AX (I/E) Access Points

The following mesh features are not supported:

- Serial backhaul AP support with separate backhaul radios for uplink and downlink.
- Public Safety channels (4.9-GHz band) support.
- Passive Beaconing (Anti-Stranding)

Note

- Only Root APs support SSO. MAPs will disconnect and rejoin after SSO.

  The AP Stateful Switch Over (SSO) feature allows the access point (AP) to establish a CAPWAP tunnel with the Active controller and share a mirror copy of the AP database with the Standby controller. The overall goal for the addition of AP SSO support to the controller is to reduce major downtime in wireless networks due to failure conditions that may occur due to box failover or network failover.
- In a mixed regulatory domain mesh AP deployment, ensure that the Dynamic Channel Assignment (DCA) allowed channel list is supported by MAPs.
- When you disable the admin state on the 2.4-GHz radio of mesh APs, and the root AP (RAP) backhaul radio is switched to 2.4-GHz, RAP will still use 2.4-GHz radio to serve the mesh backhaul connections, inspite of 2.4-GHz radio being in the disabled state.

MAC Authorization

You must enter the MAC address of an AP in the controller to make a MAP join the controller. The controller responds only to those CAPWAP requests from MAPs that are available in its authorization list. Remember to use the MAC address provided at the back of the AP.

MAC authorization for MAPs connected to the controller over Ethernet occurs during the CAPWAP join process. For MAPs that join the controller over radio, MAC authorization takes place when the corresponding AP tries to secure an adaptive wireless path protocol (AWPP) link with the parent MAP. The AWPP is the protocol used in Cisco mesh networks.

The Cisco Catalyst 9800 Series Wireless Controller supports MAC authorization internally as well as using an external AAA server.

Preshared Key Provisioning

Customers with mesh deployments can see their MAPs moving out of their network and joining another mesh network when both these mesh deployments use AAA with wild card MAC filtering to allow the association of MAPs. Since MAPs might use EAP-FAST, this cannot be controlled because a security combination of MAC address and type of AP is used for EAP, and no controlled configuration is available. The preshared key (PSK) option with a default passphrase also presents a security risk.

This issue is prominently seen in overlapping deployments of two service providers when the MAPs are used in a moving vehicle (public transportation, ferry, ship, and so on.). This way, there is no restriction on MAPs to remain with the service providers' mesh network, and MAPs can get hijacked or getting used by another service provider's network and cannot serve the intended customers of the original service providers in the deployment.

The PSK key provisioning feature enables a PSK functionality from the controller which helps make a controlled mesh deployment and enhance MAPs security beyond the default one. With this feature the MAPs that are configured with a custom PSK, will use the PSK key to do their authentication with their RAPs and controller.

EAP Authentication

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally on the controller. It is designed for use in remote offices that want to maintain connectivity with wireless clients when the backend system gets disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, which in turn, removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports only the EAP-FAST authentication method for MAP authentication between the controller and wireless clients.

Local EAP uses an LDAP server as its backend database to retrieve user credentials for MAP authentication between the controller and wireless clients. An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user.

Note If RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if RADIUS servers are not found, timed out, or were not configured.

EAP Authentication with LSC

Locally significant certificate-based (LSC-based) EAP authentication is also supported for MAPs. To use this feature, you should have a public key infrastructure (PKI) to control certification authority, define policies, validity periods, and restrictions and usages on the certificates that are generated, and get these certificates installed on the APs and controller.

After these customer-generated certificates or LSCs are available on the APs and controller, the devices can start using these LSCs, to join, authenticate, and derive a session key.

LSCs do not remove any preexisting certificates from an AP. An AP can have both LSC and manufacturing installed certificates (MIC). However, after an AP is provisioned with an LSC, the MIC certificate is not used during boot-up. A change from an LSC to MIC requires the corresponding AP to reboot.

The controller also supports mesh security with EAP authentication to a designated server in order to:

- Authenticate the mesh child AP
- Generate a master session key (MSK) for packet encryption.

Bridge Group Names

Bridge group names (BGNs) control the association of MAPs to the parent mesh AP. BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one RAP in your network in the same sector (area). BGN is a string comprising a maximum of 10 characters.

A BGN of *NULL VALUE* is assigned by default during manufacturing. Although not visible to you, it allows a MAP to join the network prior to your assignment of your network-specific BGN.

If you have two RAPs in your network in the same sector (for more capacity), we recommend that you configure the two RAPs with the same BGN, but on different channels.

When Strict Match BGN is enabled on a MAP, it will scan ten times to find a matching BGN parent. After ten scans, if the AP does not find the parent with matching BGN, it will connect to the nonmatched BGN and maintain the connection for 15 minutes. After 15 minutes, the AP will again scan ten times, and this cycle continues. The default BGN functionalities remain the same when Strict Match BGN is enabled.

In Cisco Catalyst 9800 Series Wireless Controller, the BGN is configured on the mesh profile. Whenever a MAP joins the controller, the controller pushes the BGN that is configured on the mesh profile to the AP.

Preferred Parent Selection

The preferred parent for a MAP enables you to enforce a linear topology in a mesh environment. With this feature, you can override the Adaptive Wireless Path Protocol-defined (AWPP-defined) parent selection mechanism and force a MAP to go to a preferred parent.

For Cisco Wave 1 APs, when you configure a preferred parent, ensure that you specify the MAC address of the actual mesh neighbor for the desired parent. This MAC address is the base radio MAC address that has the letter "f" as the final character. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:0f as the preferred parent.

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f
```

For Cisco Wave 2 APs, when you configure a preferred parent, the MAC address is the base radio MAC address that has "0x11" added to the last two characters. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:11 as the preferred parent.

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11
```

Background Scanning

Mesh background scanning improves convergence time, and reliability and stability of parent selection. With the help of the Background Scanning feature, a MAP can find and connect with a better potential parent across channels, and maintain its uplink with the appropriate parent all the time.

When background scanning is disabled, a MAP has to scan all the channels of the regulatory domain after detecting a parent loss in order to find a new parent and go through the authentication process. This delays the time taken for the mesh AP to connect back to the controller.

When background scanning is enabled, a MAP can avoid scanning across the channels to find a parent after detecting a parent loss, and select a parent from the neighbor list and establish the AWPP link.

Information About Background Scanning and MAP Fast Ancestor Find Mode

Cisco mesh access points (MAPs) are interconnected over wireless links in a tree topology. A MAP that is connected to a network through the Ethernet uplink is the root MAP, which is also known as a root access point (RAP). Adaptive Wireless Path Protocol (AWPP) is used to form the tree topology and maintain that topology. When a MAP comes up, it tries to look for another MAP (parent) to join and reach the gateway through a RAP. The same happens when a MAP loses connectivity with its existing parent. This procedure is known as mesh tree convergence.

A child MAP maintains uplink with its parent using the AWPP adjacency request/response messages that act as keepalive. If there is a consecutive loss of response messages, a parent is declared to be lost and the child MAP tries to find a new parent. A MAP maintains a list of neighbors of the current ON channel, and when the AP loses its current parent, it roams to the next best potential neighbor. If no other neighbors are found, the AP scans or seeks across all the channels or subset channels to find a parent. This is time consuming.

With the help of the Background Scanning feature, the AP avoids searching for a parent across the channel set by scanning or seeking. This feature helps the child MAP to be updated about its neighbors across all the channels, helps to switch to a neighbor of any channel, and uses that neighbor as its next parent for uplink.

Background scanning allows MAPs to save time during the scan-and-seek phase while looking for a new parent, but it does not save time on the authentication to the parent.

Enabling the MAP Fast Ancestor Finding feature enables a novel method to reduce the need for sending or receiving beacons at the network formation, while starting or deploying a new mesh network.

Note

- The Background Scanning and MAP Fast Ancestor Finding feature support in Cisco IOS XE Dublin 17.11.1, is not compatible with the legacy Background Scanning feature that is supported in the Cisco Wave 1 APs.
- When you enable Background Scanning on the APs that are not equipped with RHL radio, a performance penalty is imposed in terms of the bandwidth available in the backhaul. This performance penalty is high at system startup and lower after the system reaches the steady-state.

Mesh Backhaul at 2.4 GHz and 5 GHz

A backhaul is used to create only the wireless connection between MAPs. The backhaul interface is 802.11a/n/ac/g depending upon the AP. The default backhaul interface is 5-GHz. The rate selection is important for effective use of the available radio frequency spectrum. The rate can also affect the throughput of client devices. (Throughput is an important metric used by industry publications to evaluate vendor devices.)

Mesh backhaul is supported at 2.4-GHz and 5-GHz. However, in certain countries it is not allowed to use mesh network with a 5-GHz backhaul network. The 2.4-GHz radio frequencies allow you to achieve much larger mesh or bridge distances. When a RAP gets a slot-change configuration, it gets propagated from the RAP to all its child MAPs. All the MAPs get disconnected and join the new configured backhaul slot.

Information About Mesh Backhaul

This section provides information about mesh backhaul at 2.4-GHz. By default, the backhaul interface for mesh APs is 802.11a/ac/ax. Certain countries do not allow the use of mesh network with a 5-GHz backhaul network. Even in countries where 5-GHz is permitted, we recommend that you use 2.4-GHz radio frequencies to achieve much larger mesh or bridge distances.

The Mesh backhaul at 2.4-GHz is supported on the following access points:

- Cisco Catalyst 9124AX Series Outdoor Access Point
- Cisco Aironet 1540 Series Outdoor Access Points
- Cisco Aironet 1542D Outdoor Access Points
- Cisco Aironet 1562D Outdoor Access Points
- Cisco Aironet 1562E Outdoor Access Points
- Cisco Aironet 1562I Outdoor Access Points
- Cisco Aironet 1562PS Access Points
- Cisco Aironet 1570 Series Outdoor Access Points
- Cisco Aironet 1815i Access Points
- Cisco Aironet 1815m Series Access Point
- Cisco Aironet 1830 Series Access Points

- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 2800e Access Points
- Cisco Aironet 2800i Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Access Points
- Cisco Catalyst IW6300 DC Heavy Duty Access Point
- Cisco Catalyst IW6300 DCW Heavy Duty Access Point
- Cisco Catalyst IW6300 Series Heavy Duty Access Points
- Cisco 6300 Series Embedded Services Access Points

Note In Israel, you must ensure that you run the **ap country IO** command to enable the outdoor country code for the selected radio. After you configure using the **ap country IO** command, the 2.4-GHz radio is enabled and 5-GHz radio is disabled.

Information About Mesh Serial Backhaul

The Mesh Serial Backhaul feature in a mesh access point (MAP), allows different channels for uplink and downlink access, thus improving backhaul bandwidth and extending universal access. One radio is used as the uplink radio and a different one is used as the downlink radio. This allows the in-bound and out-bound traffic to flow through exclusive communication channels, thereby improving performance and avoiding problems associated with a shared access medium.

The Mesh Serial Backhaul feature is supported in the controller from Cisco IOS XE Cupertino 17.7.1 onwards, for Cisco Catalyst 9124AXE outdoor APs. A new knob is introduced under the radio profile, and that radio profile is associated with a radio frequency (RF) tag to enable the Mesh Serial Backhaul feature. When you enable this feature, the mesh configuration is shared by all the APs that share the same mesh profile. Radio configuration is shared by all the APs that are configured with the same radio profile.

Basic client access functionality is offered on the 2.4-GHz radio and the 5-GHz radio, which are not used in serial backhaul. Universal access is made available on the downlink radio.

Note Slot 1 and slot 0 are supported as mesh backhaul. Slot 2 is not supported as a mesh backhaul. You can utilize slot 2 for client serving or for serial backhaul downlink.

Channel Assignment

For the Mesh Serial Backhaul feature, channels are assigned according to the following rules:

- Uplink and downlink channels are different.
- All the 5-GHz radios maintain a frequency guard between their operating channels. For example, 100-MHz channel spacing between radios in Cisco Catalyst 9124AXE outdoor APs.

- Dynamic Frequency Selection (DFS) channels are supported.

In a root access point, because the uplink is wired, channels are assigned by the controller. On the other hand, a mesh access point uses the last channel configured by the controller for this radio, or uses the default channel. If the channel used by MAP is not compatible with the uplink, MAP picks a valid random channel and notifies the controller. In another scenario, MAP randomly picks a new downlink channel when it receives a channel change alert on the uplink radio. MAP checks the validity of the downlink radio and picks a random channel if the current channel is not compatible.

Note Ensure that the following prerequisites are met before channel assignment:

- Enable tri-radio globally by running the **Device# ap tri-radio** command.
- Enable the dual radio on the APs by running the **Device# ap name *ap-name* dot11 5ghz dual-radio mode enable** command.

Use Cases

The following are some of the use cases for the Mesh Serial Backhaul feature.

- **Maximize Throughput**: Serial backhaul allows the 5-GHz backhaul to operate on different channels, thereby maximizing throughput over multiple mesh hops.
- **Network Segregation**: APs that have serial backhaul enabled, segregate backhaul channel on mesh topographies. This is efficient because it avoids localized link interferences.

Information About Mesh Backhaul RRM

Root access points (RAPs) choose backhaul channels to operate in mesh networks. Until Cisco IOS XE Cupertino 17.8.1, this operation occurred by an explicit configuration, a least congested scan during RAP boot time, during the initial radio resource management (RRM) run without mesh access points (MAPs) connected, or a backhaul channel that was chosen at random. As a result, a poor backhaul channel selection resulted in poor performance.

From Cisco IOS XE Cupertino 17.9.1 onwards, RRM DCA is run on mesh backhaul, in auto mode, in FlexConnect or centralized networks. For APs that do not have dedicated (RHL) radios, DCA is triggered by running commands in the privilege EXEC mode.

RRM continuously evaluates the channel conditions to ensure that the network utilizes the least congested channels. The network uses the transmission static power if it is configured, or falls back to the default level. This is supported on APs that have dedicated radios to scan channel conditions, without any user perceptible interruption to the mesh network traffic.

In the mesh backhaul RRM feature, the RRM DCA decides all the downlink channels in a steady network. However, if an AP detects a change in its uplink roam or radar detection response, the AP chooses the best downlink to converge faster.

Note APs choosing the best possible downlink is limited to serial backhaul enabled APs only.

To avoid a poor channel backhaul selection, from Cisco IOS XE Dublin 17.14.1 onwards, the RRM DCA optimizes the RAP backhaul radio channel of a mesh subtree by considering the noise, interference, load, and the RF parameter measurements only from the RAP. The RRM DCA on Mesh Backhaul feature enables DCA to make better channel assignment for a mesh subtree, by having continuous measurements and inputs from the whole mesh tree required to run DCA.

To enable RRM DCA on a full mesh tree run the **wireless mesh backhaul rrm auto-dca** command. To trigger DCA once, run the **ap dot11 [5ghz | 2.4 ghz] rrm channel-update mesh** command.

To understand what happened during a DCA run on the mesh backhaul, use the **show wireless mesh rrm dca status** and **show wireless mesh rrm dca changed** commands.

Note

- In a topology with mixed APs (RF ASIC capable and non-capable APs), only inputs from the RF ASIC capable APs apply for **auto-dca**.
- All mesh APs in a subtree should be configured to belong to the same site-tag for DCA to work properly.
- This feature is limited to RF ASIC capable APs, such as Cisco Catalyst 9124 Series APs and Cisco Catalyst 9130 Series APs.

Dynamic Frequency Selection

To protect the existing radar services, the regulatory bodies require that devices that have to share the newly opened frequency sub-band behave in accordance with the Dynamic Frequency Selection (DFS) protocol. DFS dictates that in order to be compliant, a radio device must be capable of detecting the presence of radar signals. When a radio detects a radar signal, the radio should stop transmitting for at least 30 minutes to protect that service. The radio should then select a different channel to transmit on, but only after monitoring it. If no radar is detected on the projected channel for at least one minute, the new radio service device can begin transmissions on that channel. The DFS feature allows mesh APs to immediately switch channels when a radar event is detected in any of the mesh APs in a sector.

Country Codes

Controllers and APs are designed for use in many countries having varying regulatory requirements. The radios within the APs are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

In certain countries, there is a difference in the following for indoor and outdoor APs:

- Regulatory domain code
- Set of channels supported
- Transmit power level

Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing a wireless network when attacks involving these clients are detected in Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats, including worms, spyware or adware, network viruses, and application abuse.

Mesh Interoperability Between Controllers

Interoperability can be maintained between AireOS and the Cisco Catalyst 9800 Series Wireless Controller with the following support:

- MAPs can join an AireOS controller through a mesh network formed by APs connected to a Cisco Catalyst 9800 Series Wireless Controller.
- MAPs can join a Cisco Catalyst 9800 Series Wireless Controller through a mesh network formed by APs connected to as AireOS controller.
- MAP roaming is supported between parent mesh APs connected to AireOS and the Cisco Catalyst 9800 Series Wireless Controller by using PMK cache.

Note For seamless interoperability, AireOS controller and the Cisco Catalyst 9800 Series Wireless Controller should be in the same mobility group and use the image versions that support IRCM.

Information About DHCP and NAT Functionality on Root AP (RAP)

Note This feature is applicable for Cisco Aironet 1542 series outdoor access points only.

The access points associated to a mesh network can play one of the two roles:

- Root Access Point (RAP) - An access point can be a root access point for multiple mesh networks.
- Mesh Access Point (MAP) - An access point can be a mesh access point for only one single mesh network at a time.

DHCP and NAT Functionality on Root AP - IPv4 Scenario

This feature enables the controller to send a TLV to RAP when a new RAP joins the controller.

The following covers the workflow:

- Controller pushes TLV to RAP for enabling DHCP and NAT functionality.

- Client associates to an SSID.
- RAP executes DHCP functionality to assign private IPv4 address to the client.
- RAP executes NAT functionality to get the private IPv4 address of the client and allow access to the network.

Mesh Convergence

Mesh convergence allows MAPs to reestablish connection with the controller, when it loses backhaul connection with the current parent. To improve the convergence time, each mesh AP maintains a subset of channels that is used for future scan-seek and to identify a parent in the neighbor list subset.

The following convergence methods are supported.

Table 126: Mesh Convergence

Mesh Convergence	Parent Loss Detection / Keepalive Timers
Standard	21 / 3 seconds
Fast	7 / 3 seconds
Very Fast	4 / 2 seconds
Noise-tolerant-fast	21 / 3 seconds

Noise-Tolerant Fast

Noise-tolerant fast detection is based on the failure to get a response for an AWPP neighbor request, which evaluates the current parent every 21 seconds in the standard method. Each neighbor is sent a unicast request every 3 seconds along with a request to the parent. Failure to get a response from the parent initiates either a roam if neighbors are available on the same channel or a full scan for a new parent.

Ethernet Bridging

For security reasons, the Ethernet port on all the MAPs are disabled by default. They can be enabled only by configuring Ethernet bridging on the root and its respective MAP.

Both tagged and untagged packets are supported on secondary Ethernet interfaces.

In a point-to-point bridging scenario, a Cisco Aironet 1500 Series MAP can be used to extend a remote network by using the backhaul radio to bridge multiple segments of a switched network. This is fundamentally a wireless mesh network with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access. To use an Ethernet-bridged application, enable the bridging feature on the RAP and on all the MAPs in that sector.

Ethernet bridging should be enabled for the following scenarios:

- Use mesh nodes as bridges.
- Connect Ethernet devices, such as a video camera on a MAP using its Ethernet port.

Note Ensure that Ethernet bridging is enabled for every parent mesh AP taking the path from the mesh AP to the controller.

In a mesh environment with VLAN support for Ethernet bridging, the secondary Ethernet interfaces on MAPs are assigned a VLAN individually from the controller. All the backhaul bridge links, both wired and wireless, are trunk links with all the VLANs enabled. Non-Ethernet bridged traffic, as well as untagged Ethernet bridged traffic travels along the mesh using the native VLAN of the APs in the mesh. It is similar for all the traffic to and from the wireless clients that the APs are servicing. The VLAN-tagged packets are tunneled through AWPP over wireless backhaul links.

VLAN Tagging for MAP Ethernet Clients

The backhaul interfaces of mesh APs are referred to as primary interfaces, and other interfaces are referred to as secondary interfaces.

Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

Multicast Over Mesh Ethernet Bridging Network

Mesh multicast modes determine how bridging-enabled APs such as MAP and RAP, send multicast packets among Ethernet LANs within a mesh network. Mesh multicast modes manage only non-CAPWAP multicast traffic. CAPWAP multicast traffic is governed by a different mechanism.

Three different mesh multicast modes are available to manage multicast and broadcast packets on all MAPs. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

The three mesh multicast modes are:

- Regular mode: Data is multicast across the entire mesh network and all its segments by bridging-enabled RAP and MAP.
- In-only mode: Multicast packets received from the Ethernet by a MAP are forwarded to the corresponding RAP's Ethernet network. No additional forwarding occurs, which ensures that non-CAPWAP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP to MAP multicasts do not occur because such multicasts are filtered out.
- In-out mode: The RAP and MAP both multicast but in a different manner.
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP over Ethernet, and the MAP-to-MAP packets are filtered out of the multicast.
  - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. When the in-out mode is in operation, it is important to properly

partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

Radio Resource Management on Mesh

The Radio Resource Management (RRM) software embedded in the controller acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables the controller to continually monitor the associated lightweight APs for information on traffic load, interference, noise, coverage, and other nearby APs:

The RRM measurement in the mesh AP backhaul is enabled based on the following conditions:

- Mesh AP has the Root AP role.
- Root AP has joined using Ethernet link.
- Root AP is not serving any child AP.

Air Time Fairness on Mesh

The Air Time Fairness (ATF) on Mesh feature is conceptually similar to the ATF feature for local access points (APs). ATF is a form of wireless quality of service (QoS) that regulates downlink airtime (as opposed to egress bandwidth). Before a frame is transmitted, the ATF budget for that SSID is checked to ensure that there is sufficient airtime budget to transmit the frame. Each SSID can be thought of as having a token bucket (1 token = 1 microsecond of airtime). If the token bucket contains enough airtime to transmit the frame, it is transmitted over air. Otherwise, the frame can either be dropped or deferred. Deferring a frame means that the frame is not admitted into the Access Category Queue (ACQ). Instead, it remains in the Client Priority Queue (CPQ) and transmitted at a later time when the corresponding token bucket contains a sufficient number of tokens (unless the CPQ reaches full capacity, at which point, the frame is dropped). The majority of the work involved in the context of ATF takes place on the APs. The wireless controller is used to configure the ATF on Mesh and display the results.

In a mesh architecture, the mesh APs (parent and child MAPs) in a mesh tree access the same channel on the backhaul radio for mesh connectivity between parent and child MAPs. The root AP is connected by wire to the controller, and MAPs are connected wirelessly to the controller. Hence, all the CAPWAP and Wi-Fi traffic are bridged to the controller through the wireless backhaul radio and through RAP. In terms of physical locations, normally, RAPs are placed at the roof top and MAPs in multiple hops are placed some distance apart from each other based on the mesh network segmentation guidelines. Hence, each MAP in a mesh tree can provide 100 percent of its own radio airtime downstream to its users though each MAP accessing the same medium. Compare this to a non-mesh scenario, where neighboring local-mode unified APs in the arena next to each other in different rooms, serving their respective clients on the same channel, and each AP providing 100% radio airtime downstream. ATF has no control over clients from two different neighboring APs accessing the same medium. Similarly, it is applicable for MAPs in a mesh tree.

For outdoor or indoor mesh APs, ATF must be supported on client access radios that serve regular clients similarly to how it is supported on ATF on non-mesh unified local mode APs to serve the clients. Additionally, it must also be supported on backhaul radios which bridge the traffic to/from the clients on client access radios to RAPs (one hop) or through MAPs to RAPs (multiple hops). It is a bit tricky to support ATF on the backhaul radios using the same SSID/Policy/Weight/Client fair-sharing model. Backhaul radios do not have SSIDs and it always bridge traffic through their hidden backhaul nodes. Therefore, on the backhaul radios in a RAP or

a MAP, the radio airtime downstream is shared equally, based on the number of backhaul nodes. This approach provides fairness to users across a wireless mesh network, where clients associated to second-hop MAP can stall the clients associated to first-hop MAP where second-hop MAP is connected wireless to first-hop MAP through backhaul radio even though the Wi-Fi users in the MAPs are separated by a physical location. In a scenario where a backhaul radio has an option to serve normal clients through universal client access feature, ATF places the regular clients into a single node and groups them. It also enforces the airtime by equally sharing the radio airtime downstream, based on the number of nodes (backhaul nodes plus a single node for regular clients).

Spectrum Intelligence for Mesh

The Spectrum Intelligence feature scans for non-Wi-Fi radio interference on 2.4-GHz and 5-GHz bands. The feature supports client serving mode and monitor mode. The Cisco CleanAir technology in mesh backhaul and access radios provides an Interference Device Report (IDR) and Air Quality Index (AQI). Two key mitigation features (Event-Driven Radio Resource Management [EDRRM] and Persistence Device Avoidance [PDA]) are present in CleanAir. Both rely directly on information that can only be gathered by CleanAir. In the client-access radio band, they work the same way in mesh networks as they do in non-mesh networks in the backhaul radio band, the CleanAir reports are only displayed on the controller. No action is taken through ED-RRM.

Note that no specific configuration options are available to enable or disable CleanAir for MAPs.

For more information about Spectrum Intelligence, see #unique_2120 section.

Indoor Mesh Interoperability with Outdoor Mesh

Interoperability of indoor MAPs with outdoor APs are supported. This helps to bring coverage from outdoors to indoors. However, we recommend that you use indoor MAPs for indoor use only, and deploy them outdoors only under limited circumstances such as a simple short-haul extension from an indoor WLAN to a hop in a parking lot.

Mobility groups can be shared between outdoor mesh networks and indoor WLAN networks. It is also possible for a single controller to control indoor and outdoor MAPs simultaneously. Not that the same WLANs are broadcast out of both indoor and outdoor MAPs.

Workgroup Bridge

A workgroup bridge (WGB) is used to connect wired networks over a single wireless segment by informing the corresponding MAP of all the clients that the WGB has on its wired segment via IAPP messages. In addition to the IAPP control messages, the data packets for WGB clients contain an extra MAC address in the 802.11 header (four MAC headers, versus the normal three MAC data headers). The extra MAC in the header is the address of the workgroup bridge itself. This extra MAC address is used to route a packet to and from the corresponding clients.

APs can be configured as workgroup bridges. Only one radio interface is used for controller connectivity, Ethernet interface for wired client connectivity, and other radio interface for wireless client connectivity.

In Cisco Catalyst 9800 Series Wireless Controller, WGB acts as a client association, with the wired clients behind WGB supported for data traffic over the mesh network. Wired clients with different VLANs behind WGB are also supported.

Link Test

A link test is used to determine the quality of the radio link between two devices. Two types of link-test packets are transmitted during a link test: request and response. Any radio receiving a link-test request packet fills in the appropriate text boxes and echoes the packet back to the sender with the response type set.

The radio link quality in the client-to-access point direction can differ from that in the access point-to-client direction due to the asymmetrical distribution of the transmit power and receive sensitivity on both sides. Two types of link tests can be performed: a ping test and a CCX link test.

With the ping link test, the controller can test link quality only in the client-to-access point direction. The RF parameters of the ping reply packets received by the access point are polled by the controller to determine the client-to-access point link quality.

With the CCX link test, the controller can also test the link quality in the access point-to-client direction. The controller issues link-test requests to the client, and the client records the RF parameters (received signal strength indicator [RSSI], signal-to-noise ratio [SNR], and so on). of the received request packet in the response packet. Both the link-test requestor and responder roles are implemented on the access point and controller. Not only can the access point or controller initiate a link test to a CCX v4 or v5 client, but a CCX v4 or v5 client can initiate a link test to the access point or controller.

Mesh Daisy Chaining

Mesh APs have the capability to *daisy chain* APs when they function as MAPs. The *daisy chained* MAPs can either operate the APs as a serial backhaul, allowing different channels for uplink and downlink access, thus improving backhaul bandwidth, or extend universal access. Extending universal access allows you to connect a local mode or FlexConnect mode Mesh AP to the Ethernet port of a MAP, thus extending the network to provide better client access.

Daisy chained APs must be cabled differently depending on how the APs are powered. If an AP is powered using DC power, an Ethernet cable must be connected directly from the LAN port of the Primary AP to the PoE in a port of the Subordinate AP.

The following are the guidelines for the daisy chaining mode:

- Primary MAP should be configured as mesh AP.
- Subordinate MAP should be configured as root AP.
- Daisy chaining should be enabled on both primary and subordinate MAP.
- Ethernet bridging should be enabled on all the APs in the Bridge mode. Enable Ethernet bridging in the mesh profile and map all the bridge mode APs in the sector to the same mesh profile.
- VLAN support should be enabled on the wired root AP, subordinate MAP, and primary MAP along with proper native VLAN configuration.

Mesh Leaf Node

You can configure a MAP with lower performance to work only as a leaf node. When the mesh network is formed and converged, the leaf node can only work as a child MAP, and cannot be selected by other MAPs as a parent MAP, thus ensuring that the wireless backhaul performance is not downgraded.

Flex+Bridge Mode

Flex+Bridge mode is used to enable FlexConnect capabilities on mesh (bridge mode) APs. Mesh APs inherit VLANs from the root AP that is connected to it.

Any EWC capable AP in Flex mode connected to a MAP, should be in CAPWAP mode (AP-type CAPWAP).

You can enable or disable VLAN trunking and configure a native VLAN ID on each AP for any of the following modes:

- FlexConnect
- Flex+Bridge (FlexConnect+Mesh)

Backhaul Client Access

When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. The backhaul radio can be a 2.4-GHz or 5-GHz radio. This means that a backhaul radio can carry both backhaul traffic and client traffic.

When Backhaul Client Access is disabled, only backhaul traffic is sent over the backhaul radio, and client association is performed only over the access radio.

Note Backhaul Client Access is disabled by default. After the Backhaul Client Access is enabled, all the MAPs, except subordinate AP and its child APs in daisy-chained deployment, reboot.

Mesh CAC

The Call Admission Control (CAC) enables a mesh access point to maintain controlled quality of service (QoS) on the controller to manage voice quality on the mesh network. Bandwidth-based, or static CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call. Each access point determines whether it is capable of accommodating a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If there is not enough bandwidth available to maintain the maximum allowed number of calls with acceptable quality, the mesh access point rejects the call.

- When client roams from one MAP to another in same site, bandwidth availability is checked again in the new tree for the active calls.

- When MAP roams to new parent, the active calls are not terminated and it continues to be active with other active calls in the sub tree.
- High Availability (HA) for MAPs is not supported; calls attached to MAP's access radio are terminated on HA switchover.
- HA for RAP is supported, hence calls attached to RAP's access radio continues to be active in new controller after switchover.
- Mesh CAC algorithm is applicable only for voice calls.
- For Mesh backhaul radio bandwidth calculation, static CAC is applied. Load-based CAC is not used as the APs do not support load-based CAC in Mesh backhaul.
- Calls are allowed based on available bandwidth on a radio. Airtime Fairness (ATF) is not accounted for call admission and the calls that fall under ATF policy are given bandwidth as per ATF weight.

Mesh CAC is not supported for the following scenarios.

- APs in a Mesh tree assigned with different site tags.
- APs in a Mesh tree assigned with the default site tag.

Prerequisites for Mesh Ethernet Daisy Chaining

- Ensure that you have configured the AP role as root AP.
- Ensure that you have enabled Ethernet Bridging and Strict Wired Uplink on the corresponding AP.
- Ensure that you have disabled VLAN transparency.
- To enable VLAN support on each root AP for bridge mode APs, use the **ap name** *name-of-rap* **mesh vlan-trunking [native]** *vlan-id* command to configure a trunk VLAN on the corresponding RAP.
- To enable VLAN support on each root AP, for Flex+Bridge APs, you must configure the native VLAN ID under the corresponding flex profile.
- Ensure that you use a 4-pair cables that support 1000 Mbps. This feature does not work properly with 2-pair cables supporting 100 Mbps.

Restrictions for Mesh Ethernet Daisy Chaining

- This feature is applicable to the Cisco Industrial Wireless 3702 AP and Cisco Catalyst 9124 Series APs.
- This feature is applicable to APs operating in Bridge mode and Flex+Bridge mode only.
- In Flex+Bridge mode, if local switching WLAN is enabled, the work group bridge (WGB) multiple VLAN is not supported.
- To support the Ethernet daisy chain topology, you must not connect the Cisco Industrial Wireless 3702 PoE out port to other Cisco Industrial Wireless 3702 PoE in the port, and the power injector must be used as power supply for the AP.

- The network convergence time increases when the number of APs increase in the chain.
- Any EWC capable AP which is part of daisy chaining and has been assigned the RAP role, must be in CAPWAP mode (ap-type capwap).

Speeding up Mesh Network Recovery Through Fast Detection of Uplink Gateway Reachability Failure

In all 802.11ac Wave 2 APs, the speed of mesh network recovery mechanism is increased through fast detection of uplink gateway reachability failure. The uplink gateway reachability of the mesh APs is checked using ICMP ping to the default gateway, either IPv4 or IPv6.

Mesh AP triggers the reachability check in the following two scenarios:

- After a new uplink is selected, until the mesh AP joins the controller

  After a new uplink is selected, the mesh AP has a window of 45 seconds to reach gateway (via static IP or DHCP) through the selected uplink. If the mesh AP still fails to reach the gateway after 45 seconds, the current uplink is in blocked list and the uplink selection process is restarted. If the AP joins the controller within this 45-second window, the reachability check is stopped. Subsequently, there is no gateway reachability check during normal operations.

- As soon as the mesh AP times out its connection with the controller

  After the mesh AP times out its connection with the controller and the AP fails to reach the gateway in 5 seconds, the current uplink is immediately added to the blocked list and the uplink selection process is restarted.

Fast Teardown for a Mesh Deployment

In mesh deployments, sometimes a root access point connects to the controller through a nonreliable link such as a wireless microwave link. If a data uplink failure occurs, client loses connectivity to detect the cause of the failure. The feature allows you to detect the root access point uplink failure faster in a mesh deployment and address fast teardown of the mesh network when uplink failure occurs on the root access point.

Note Fast Teardown for Mesh APs is not supported on Cisco Industrial Wireless (IW) 3702 Access Points.

Configuring MAC Authorization (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Advanced** > **Device Authentication**.

Step 2 Click **Add**.

The **Quick Step: MAC Filtering** window is displayed.

Step 3 In the **Quick Step: MAC Filtering** window, complete the following:

a) Enter the **MAC Address**. The MAC address can be in either *xx:xx:xx:xx:xx:xx*, *xx-xx-xx-xx-xx-xx*, or *xxxx.xxxx.xxxx* format.
b) Choose the **Attribute List Name** from the drop-down list.
c) Choose the **WLAN Profile Name** from the drop-down list.
d) Click **Apply to Device**.

Step 4 Choose **Configuration** > **Security** > **AAA** > **AAA Method List** > **Authorization**.

Step 5 Click **Add**.
The **Quick Step: AAA Authorization** window is displayed.

Step 6 In the **Quick Step: AAA Authorization** window, complete the following:

a) Enter the **Method List Name**.
b) Choose the **Type** from the drop-down list.
c) Choose the **Group Type** from the drop-down list.
d) Check the **Fallback to Local** check box.
e) Check the **Authenticated** check box.
f) Move the required servers from the **Available Server Groups** to the **Assigned Server Groups.**
g) Click **Apply to Device**.

Step 7 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 8 Click the mesh profile.
The **Edit Mesh Profile** window is displayed.

Step 9 Click the **Advanced** tab.

Step 10 In the **Security** settings, from the **Method** drop-down list, choose **EAP**.

Step 11 Choose the **Authentication Method** from the drop-down list.

Step 12 Choose the **Authorization Method** from the drop-down list.

Step 13 Click **Update & Apply to Device**.

Configuring MAC Authorization (CLI)

Follow the procedure given below to add the MAC address of a bridge mode AP to the controller.

Before you begin

- MAC filtering for bridge mode APs are enabled by default on the controller. Therefore, only the MAC address need to be configured. The MAC address that is to be used is the one that is provided at the back of the corresponding AP.
- MAC authorization is supported internally, as well as using an external AAA server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**username** *user-name* **Example:** `Device(config)# username username1`	Configures user name authentication for MAC filtering where username is MAC address.
Step 3	**aaa authorization credential-download** *method-name* **local** **Example:** `Device(config)# aaa authorization credential-download list1 local`	Sets an authorization method list to use local credentials.
Step 4	**aaa authorization credential-download** *method-name* **radius group** *server-group-name* **Example:** `Device(config)# aaa authorization credential-download auth1 radius group radius-server-1`	Sets an authorization method list to use a RADIUS server group.
Step 5	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 6	**method authorization** *method-name* **Example:** `Device(config-wireless-mesh-profile)# method authorization auth1`	Configures the authorization method for mesh AP authorization.

Configuring MAP Authorization - EAP (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Method List** > **Device Authentication**.

Step 2 Click **Add**.

Step 3 Enter **Method List Name**.

Step 4 Choose **Type** as dot1x and **Group Type** from the drop-down lists.

dot1x

Step 5 Check or uncheck the **Fallback to Local** check box.

Step 6 Move the required servers from the **Available Server Groups** to the **Assigned Server Groups.**

Step 7 Click **Apply to Device**.

Step 8 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 9 Click the mesh profile. The **Edit Mesh Profile** window is displayed.

Step 10 Choose the **Advanced** tab.

Step 11 In the **Security** settings, from the **Method** drop-down list, choose **EAP**.

Step 12 Choose the options from the **Authentication Method** and **Authorization Method** drop-down lists.

Step 13 Click **Update & Apply to Device**.

Configuring MAP Authorization (CLI)

Select and configure authentication method of EAP/PSK for MAP authentication.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication** *method-name* **radius group** *server-group-name* **Example:** `Device(config)# aaa authentication dot1x auth1 radius group radius-server-1`	For local authentication: `Device(config)# aaa authentication dot1x auth1 local` Sets an authentication method list to use a RADIUS server group. This is required for EAP authentication.
Step 3	**wireless profile mesh** *profile--name* **local** **Example:** `Device(config)# wireless profile mesh mesh1`	Sets an authorization method list to use local credentials.
Step 4	**security eap** *server-group-name* **Example:** `Device(config-wireless-mesh-profile)# security eap / psk`	Configures the mesh security EAP/PSK for mesh AP.
Step 5	**method authentication** *method-name* **Example:** `Device(config-wireless-mesh-profile)# method authentication auth1`	Configures the authentication method for mesh AP authentication.

Configuring PSK Provisioning (CLI)

When PSK provisioning is enabled, the APs join with default PSK initially. After that PSK provisioning key is set, the configured key is pushed to the newly joined AP.

Follow the procedure given below to configure a PSK:

Before you begin

The provisioned PSK should have been pushed to all the APs that are configured with PSK as mesh security.

Note

- PSKs are saved across reboots in the controller as well as on the corresponding mesh AP.
- A controller can have total of five PSKs and one default PSK.
- A mesh AP deletes its provisioned PSK only on factory reset.
- A mesh AP never uses the default PSK after receiving the first provisioned PSK.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh security psk provisioning** **Example:** `Device(config)# wireless mesh security psk provisioning`	Configures the security method for wireless as PSK. **Note** The provisioned PSK is pushed only to those APs that are configured with PSK as the mesh security method.
Step 3	**wireless mesh security psk provisioning key** *index* {**0** | **8**} *pre-shared-key description* **Example:** `Device(config)# wireless mesh security psk provisioning key 1 0 secret secret-key`	Configures a new PSK for mesh APs.
Step 4	**wireless mesh security psk provisioning default-psk** **Example:** `Device(config)# wireless mesh security psk provisioning default-psk`	Enables default PSK-based authentication.

	Command or Action	Purpose
Step 5	**wireless mesh security psk provisioning inuse** *index* **Example:** `Device(config)# wireless mesh security psk provisioning inuse 1`	Specifies the PSK to be actively used. **Note** You should explicitly set the in-use key index in the global configuration pointing to the PSK index.

Configuring a Bridge Group Name (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In the **Advanced** tab, under the **Bridge Group** settings, enter the **Bridge Group Name**.

Step 4 Under the **Bridge Group** settings, check the **Strict Match** check box to enable the feature. When Strict Match BGN is enabled on a MAP, it scans ten times to find a matching BGN parent.

Step 5 Click **Apply to Device**.

Configuring a Bridge Group Name (CLI)

- If a bridge group name (BGN) is configured on a mesh profile, whenever a MAP joins the controller, it pushes the BGN configured on the mesh profile to the AP.
- Whenever a mesh AP moves from AireOS controller to the Cisco Catalyst 9800 Series Wireless Controller, the BGN configured on the mesh profile is pushed to that AP and stored there.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**bridge-group name** *bridge-grp-name* **Example:**	Configures a bridge group name.

	Command or Action	Purpose
	`Device(config-wireless-mesh-profile)# bridge-group name bgn1`	
Step 4	**bridge-group strict-match** **Example:** `Device(config-wireless-mesh-profile)# bridge-group strict-match`	Configures bridge group strict matching.

Configuring Background Scanning (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Choose a profile.

Step 3 In **General** tab, check the **Background Scanning** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Background Scanning

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**background-scanning** **Example:** `Device(config-wireless-mesh-profile)# background-scanning`	Configures background scanning in mesh deployments.

Configuring AP Fast Ancestor Find Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 2 Click **Add**.
The **Add Mesh Profile** window is displayed.

Step 3 In the **Add Mesh Profile** window, click the **General** tab.

Step 4 In the **Name** field, enter the mesh profile name.

Step 5 In the **Description** field, enter a description for the mesh profile.

Step 6 Check the **MAP Fast Ancestor Find** check box to enable a MAP (child) to synchronize with any neighbor MAP (parent) across all channels.

Step 7 Click **Apply to Device** to save the configuration.

Configuring Background Scanning and MAP Fast Ancestor Find Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device# wireless profile mesh default-mesh-profile`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**background-scanning** **Example:** `Device(config-wireless-mesh-profile)# background-scanning`	Configures background scanning in mesh deployments. **Note** In Cisco Catalyst 9124 Series Access Points, a dedicated RF ASIC radio is used for background scanning.
Step 4	**map-fast-ancestor-find** **Example:**	Configures fast ancestor find mode.

	Command or Action	Purpose
	`Device(config-wireless-mesh-profile)# map-fast-ancestor-find`	

Configuring Backhaul Client Access (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Choose a profile.

Step 3 In **General** tab, check the **Backhaul Client Access** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Backhaul Client Access (CLI)

Note Backhaul client access is disabled by default. After it is enabled, all the MAPs, except subordinate AP and its child APs in daisy-chained deployment, reboot.

Follow the procedure given below to enable backhaul client access on a mesh profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**client-access** **Example:** `Device(config-wireless-mesh-profile)# client-access`	Configures backhaul with client access AP.

Configuring Dot11ax Rates on Mesh Backhaul Per Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.
The **All Access Points** section, which lists all the configured APs in the network, is displayed with their corresponding details.

Step 2 Click the configured mesh AP.
The **Edit AP** window is displayed.

Step 3 Choose the **Mesh** tab.

Step 4 In the **General** section, under the **Backhaul** section, the default **Backhaul Radio Type**, **Backhaul Slot ID**, and **Rate Types** field details are displayed. Note that the values for **Backhaul Radio Type** and **Backhaul Slot ID** can be changed only for a root AP.

Step 5 From the **Rate Types** drop-down list, choose the backhaul rate type.

Based on the choice, enter the details for the corresponding fields that are displayed. The backhaul interface varies between auto and 802.11a/b/g/n/ac/ax rates depending upon the AP. Cisco Catalyst 9124AX Outdoor Access Point is the only AP that support 11ax backhaul rates on the mesh backhaul.

Step 6 In the **Backhaul MCS Index** field, enter the Modulation Coding Scheme (MCS) rate, that can be transmitted between the APs. The valid range is from 0 to 11, on both the bands.

Step 7 In the **Spatial Stream** field, enter the number of spatial streams that are supported. The maximum number of spatial streams supported on a single radio in a 5-GHz radio band is 8, while 2.4-GHz radio band supports 4 spatial streams.

Step 8 Click **Update and Apply to Device**.

Configuring Dot11ax Rates on Mesh Backhaul in Mesh Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 2 Click **Add**.
The **Add Mesh Profile** window is displayed.

Step 3 In the **Add Mesh Profile** window, click the **General** tab.

Step 4 In the **Name** field, enter the mesh profile name.

Step 5 Click the **Advanced** tab.

Step 6 In the **5 GHz Band Backhaul** section and the **2.4 GHz Band Backhaul** section, choose the **dot11ax** backhaul rate type from **Rate Types** the drop-down list.

Note Cisco Catalyst 9124AXI/D Series outdoor Access Point is the only AP to support 11ax backhaul rates on the mesh backhaul.

Step 7 In the **Dot11ax MCS index** field, specify the MCS rate at which data can be transmitted between the APs. The value range is between 0 to 11, on both the radio bands.

Step 8 In the **Spatial Stream** field, enter a value. The maximum number of spatial streams supported on a single radio in a 5-GHz radio band is 8, while 2.4- GHz radio band supports 4 spatial streams.

Step 9 Click **Update and Apply to Device**.

Configuring Wireless Backhaul Data Rate (CLI)

Backhaul is used to create a wireless connection between APs. A backhaul interface can be 802.11bg/a/n/ac depending on the AP. The rate selection provides for effective use of the available RF spectrum. Data rates can also affect the RF coverage and network performance. Lower data rates, for example, 6 Mbps, can extend farther from the AP than can have higher data rates, for example, 1300 Mbps. As a result, the data rate affects cell coverage, and consequently, the number of APs required.

Note You can configure backhaul data rate, preferably, through the mesh profile. In certain cases, where a specific data rate is needed, use the command to configure the data rate per AP.

Follow the procedure given below to configure wireless backhaul data rate in privileged EXEC mode or in mesh profile configuration mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh backhaul rate** {**auto** | **dot11abg** | **dot11ac** |**dot11n**} **Example:** `Device# #ap name ap1 mesh backhaul rate auto`	Configures backhaul transmission rate.
Step 3	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.

	Command or Action	Purpose
Step 4	**backhaul rate dot11** {**24ghz** | **5ghz**}**dot11n RATE_6M** **Example:** `Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11n mcs 31`	Configures backhaul transmission rate. **Note** Note that the rate configured on the AP (step 2) should match with the rate configured on the mesh profile (step4).

Configuring Data Rate Per AP (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **mesh backhaul rate dot11ax mcs** *<0-11>* **ss** *<1-8>* **Example:** `Device# ap name ap1 mesh backhaul rate dot11ax 5 ss 4`	Configures mesh backhaul 11ax rates for 2.4-GHz and 5-GHz bands.

Configuring Data Rate Using Mesh Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**backhaul rate dot11** {**24ghz** | **5ghz**}**dot11ax mcs** *<0-11>* **spatial-stream** *<1-8>* **Example:** `Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11ax mcs 5`	Configures backhaul transmission rate for 2.4-GHz band and 5-GHz band. The 802.11ax spatial stream value for 2.4-GHz band is from 1 to 4, and the spatial stream value for the 5-GHz band is from 1to 8.

	Command or Action	Purpose
	`spatial-stream 6` `Device(config-wireless-mesh-profile)# backhaul rate dot11 24ghz dot11ax mcs 5 spatial-stream 4`	

Configuring Mesh Backhaul (CLI)

This section describes how to configure mesh backhaul at 2.4 GHz.

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap_name* **mesh backhaul radio dot11** *24ghz* **Example:** `Device # ap name test-ap mesh backhaul radio dot11 24ghz`	Changes the mesh backhaul to 2.4 GHz.

Configuring Dynamic Frequency Selection (CLI)

DFS specifies the types of radar waveforms that should be detected along with certain timers for an unlicensed operation in the DFS channel.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**full-sector-dfs** **Example:**	Enables DFS.

	Command or Action	Purpose
	`Device(config-wireless-mesh-profile)# full-sector-dfs`	**Note** DFS functionality allows a MAP that detects a radar signal to transmit that up to the RAP, which then acts as if it has experienced radar and moves the sector. This process is called the coordinated channel change. The coordinated channel change is always enabled for Cisco Wave 2 and the later versions. The coordinated channel change can be disabled only for Cisco Wave 1 APs.

Configuring the Intrusion Detection System (CLI)

When enabled, the intrusion detection system generates reports for all the traffic on the client access. However, this is not applicable for the backhaul traffic.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**ids** **Example:** `Device(config-wireless-mesh-profile)# ids`	Configures intrusion detection system reporting for mesh APs.

Configuring Ethernet Bridging (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In **General** tab, enter the **Name** of the mesh profile.

Step 4 In the **Advanced** tab, check the **VLAN Transparent** check box to enable VLAN transparency.

Step 5 In **Advanced** tab, check the **Ethernet Bridging** check box.

Step 6 Click **Apply to Device**.

Configuring Ethernet Bridging (CLI)

The Ethernet port on the MAPs are disabled by default. It can be enabled only by configuring Ethernet bridging on the Root AP and the other respective MAPs.

Ethernet bridging can be enabled for the following scenarios:

- To use the mesh nodes as bridges.
- To connect Ethernet devices, such as a video camera, on a MAP using the MAP's Ethernet port.

Before you begin

- Ensure that you configure the following commands under the mesh profile configuration for Ethernet bridging to be enabled:
  - **ethernet-bridging**: Enables the Ethernet Bridging feature on an AP.
  - **no ethernet-vlan-transparent**: Makes the wireless mesh bridge VLAN aware. Allows VLAN filtering with the following AP command: **[no] mesh ethernet** {**0** | **1** | **2** | **3**} **mode trunk vlan allowed**.

Note If you wish to have all the VLANs bridged (where bridge acts like a piece of wire), then you must enable VLAN transparency, which allows all VLANS to pass. If you choose to use VLAN transparent mode, it is best to filter the VLANS on the wired side of the network to avoid unnecessary traffic from flooding the network.

- The switch port to which the Root AP is connected should be configured as the trunk port for Ethernet bridging to work.
- For Bridge mode APs, use the **ap name** *name-of-rap* **mesh vlan-trunking native** *vlan-id* command to configure a trunk VLAN on the corresponding RAP. The Ethernet Bridging feature will not be enabled on the AP without configuring this command.
- For FlexConnect+Brigde APs, configure the native VLAN ID under the corresponding flex profile.

Note To ensure that the MAPs apply the Ethernet VLAN configuration on the controller, configure the native VLAN on the RAP by running the following command:

```
Device# ap name ap-name no mesh vlan-trunking
Device# ap name ap-name mesh vlan-trunking native 247
```

Alternatively, you can configure native VLAN on the RAP and then the MAP in the following order:

```
Device# ap name ap-name no mesh vlan-trunking
Device# ap name ap-name mesh vlan-trunking native vlan_id
Device# ap name ap-name mesh ethernet 1 mode trunk vlan native native
Device# ap name ap-name mesh ethernet 0 mode trunk vlan allowed allowed
```

To verify the status of RAP and MAP, run the following command:

```
Device# show mesh forwarding all
```

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode access** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode access 21`	Configures the Ethernet port of the AP and sets the mode as trunk.
Step 3	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode trunk vlan native 21`	Sets the native VLAN for the trunk port.
Step 4	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan allowed** *vlan-id* **Example:** `Device# ap name ap1 mesh ethernet 1 mode trunk vlan allowed 21`	Configures the allowed VLANs for the trunk port. Permits VLAN filtering on an ethernet port of any Mesh or Root Access Point. Active only when VLAN transparency is disabled in the mesh profile.

Configuring Multicast Modes over Mesh

- If multicast packets are received at a MAP over Ethernet, they are sent to the RAP. However, they are not sent to other MAPs. MAP-to-MAP packets are filtered out of the multicast.

- If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks.
- The *in-out* mode is the default mode. When this *in-out* mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment, and then sent back into the network.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**multicast** {**in-only** | **in-out** | **regular**} **Example:** `Device(config-wireless-mesh-profile)# multicast regular`	Configures mesh multicast mode.

Configuring RRM on Mesh Backhaul (CLI)

The RRM measurement in the mesh AP backhaul is enabled based on the following conditions:

- Mesh AP has the Root AP role.
- Root AP has joined using an Ethernet link.
- Root AP is not serving any child AP.

Follow the procedure given below to enable RRM in the mesh backhaul:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh backhaul rrm** **Example:** `Device(config)# wireless mesh backhaul rrm`	Configures RRM on the mesh backhaul.

Configuring RRM Channel Assignment for Root Access Points Globally

Before you begin

Ensure that you have configured RRM for mesh backhaul before RRM DCA is triggered.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh backhaul rrm** **Example:** `Device(config)# wireless mesh backhaul rrm`	Configures RRM for mesh backhaul.
Step 3	(Optional) **wireless mesh backhaul rrm auto-dca** **Example:** `Device(config)# wireless mesh backhaul rrm auto-dca`	Configures auto DCA for RF Application Specific Integrated Circuit (ASIC) integrated RAPs.

To configure the initial channel assignment of the RAP in privileged EXEC mode through RRM, and to initiate channel selection for each bridge group, complete the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel-update mesh** **Example:** `Device# ap dot11 5ghz rrm channel-update mesh`	Initiates update of the 802.11, 802.11a, or 802.11b channel selection for every mesh Cisco AP.

	Command or Action	Purpose
Step 3	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel-update mesh bridge-group** *bridge-group-name* **Example:** `Device# ap dot11 5ghz rrm channel-update mesh bridge-group cisco-bridge-group`	Initiates update of the 802.11, 802.11a, or 802.11b channel selection for mesh AP in the bridge group.

Configuring RRM Channel Assignment for an Access Point

To trigger RRM DCA for an AP, complete the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco-ap-name* **dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel update mesh** **Example:** `Device# ap name Cisco-ap-name dot11 5ghz rrm channel update mesh`	Triggers RRM DCA for the specific AP.

Selecting a Preferred Parent (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the Access Point.

Step 3 In the **Mesh** tab, enter the **Preferred Parent MAC**.

Step 4 Click **Update & Apply to Device**.

Selecting a Preferred Parent (CLI)

Follow the procedure given below to configure a preferred parent for a MAP.

Using this mechanism, you can override the AWPP-defined parent selection mechanism and force a mesh AP to go to a preferred parent.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.

Step 2	**ap name** *ap-name* **mesh parent preferred** *mac-address*
	Example:
	`Device# ap name ap1 mesh parent preferred 00:0d:ed:dd:25:8F`
		Configures mesh parameters for the AP and sets the mesh-preferred parent MAC address.
		Note Ensure that you use the radio MAC address of the preferred parent.
		For Cisco Wave 1 APs, when you configure a preferred parent, ensure that you specify the MAC address of the actual mesh neighbor for the desired parent. This MAC address is the base radio MAC address that has the letter "f" as the final character. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:0f as the preferred parent.
		`Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f`
		For Cisco Wave 2 APs, when you configure a preferred parent, the MAC address is the base radio MAC address that has "0x11" added to the last two characters. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:11 as the preferred parent.
		`Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11`

Changing the Role of an AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the **Access Point**.

Step 3 In the **Mesh** tab, choose **Root** or **Mesh** from the **Role** drop-down list.

Step 4 Click **Update & Apply to Device**.

After the role change is triggered, the AP reboots.

Changing the Role of an AP (CLI)

Follow the procedure to change the AP from MAP to RAP or vice-versa.

By default, APs join the controller in a mesh AP role.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **role** {**mesh-ap** | **root-ap**} **Example:** `Device# #ap name ap1 root-ap`	Changes the role for the Cisco bridge mode APs. After the role change is triggered, the AP reboots.

Configuring the Mesh Leaf Node (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**ap name** *ap-name* **mesh block-child** **Example:** `Device# #ap name ap1 mesh block-child`	Sets the AP to work only as a leaf node. This AP cannot be selected by other MAPs as a parent MAP. **Note** Use the **no** form of this command to change it to a regular AP.

Configuring the Mesh Leaf Node (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 Click the Access Point.

Step 3 In the **Mesh** tab, check the **Block Child** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Subset Channel Synchronization

All the channels used by all the RAPs in a controller are sent to all the MAPs for future seek and convergence. The controller keeps a list of the subset channels for each Bridge Group Name (BGN). The list of subset channels are also shared across all the controllers in a mobility group.

Subset channel list is list of channels where RAP of particular BGN are operating. This list is communicated to all the MAPs within and across the controllers. The idea of subset channel list is for faster convergence of the Mesh APs. Convergence method can be selected in mesh profile. If the convergence method is not standard then subset channel list is pushed to MAPs.

Follow the procedure given below to configure subset channel synchronization for mobility group.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh subset-channel-sync mac** **Example:** `Device(config)# wireless mesh subset-channel-sync`	Configures subset channel synchronization for a mobility group.

Provisioning LSC for Bridge-Mode and Mesh APs (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **LSC Provision**.

Step 2 In the **Add APs to LSC Provision List** settings, click the **Select File** option to upload a CSV file that contains AP details.

Step 3 Click **Upload File**.

Step 4 You can also use the **AP MAC Address** field to search for APs using the MAC address and add them. The APs added to the provision list are displayed in the **APs in Provision List** list.

Step 5 Click **Apply**.

Step 6 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 7 Click **Add**.

Step 8 In the **General** tab, enter the **Name** of the mesh profile and check the **LSC** check box.

Step 9 In the **Advanced** tab, under the **Security** settings, choose the authorization method from the **Authorization Method** drop-down list.

Step 10 Click **Apply to Device**.

Provisioning LSC for Bridge-Mode and Mesh APs

- Configuring Locally Significant Certificate (LSC) will not remove pre-existing certificates from an AP.
- An AP can have both LSC and Message Integrity Check (MIC) certificates. However, when an AP is provisioned with LSC, the MIC certificate is not used on boot-up. A change from LSC to MIC requires the AP to reboot.

Follow the procedure given below to configure LSC for bridge-mode and mesh APs:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap lsc-provision** **Example:** `Device(config)# ap lsc-provision`	Configures LSC provisioning on an AP. **Note** This step is applicable only for mesh APs.
Step 3	**ap lsc-provision provision-list** **Example:**	(Optional) Configures LSC provision for all the APs in the provision list.

	Command or Action	Purpose
	`Device(config)# ap lsc-provision provision-list`	
Step 4	**aaa authentication dot1x** *auth-list* **radius group** *radius-server-grp* **Example:** `Device(config)# aaa authentication dot1x list1 radius group sg1`	Configures named authorization list for downloading EAP credential from radius group server.
Step 5	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 6	**lsc-only-auth** **Example:** `Device(config-wireless-mesh-profile)# lsc-only-auth`	Configures mesh security to LSC-only MAP authentication. After this command is run, all the mesh APs reboot.
Step 7	**method authorization** *local* **Example:** `Device(config-wireless-mesh-profile)# method authorization list1`	Configures an authorization method for mesh AP authorization.

Specifying the Backhaul Slot for the Root AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Click **Add**.

Step 3 In **General** tab, enter the **Name** of the mesh profile.

Step 4 In **Advanced** tab, choose the rate types from the **Rate Types** drop-down list for **5 GHz Band Backhaul** and **2.4 GHz Band Backhaul**.

Step 5 Click **Apply to Device**.

Specifying the Backhaul Slot for the Root AP (CLI)

Follow the procedure given below to set the mesh backhaul rate.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *rap-name* **mesh backhaul radio dot11**{**24ghz** | **5ghz**} [**slot** *slot-id*] **Example:** `Device# ap name rap1 mesh backhaul radio dot11 24ghz slot 2`	Sets the mesh backhaul radio slot.

Using a Link Test on Mesh Backhaul (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **AP Statistics** > **General**.

Step 2 Click the Access Point.

Step 3 Choose **Mesh** > **Neighbor** > **Linktest**.

Step 4 Choose the desired values from the **Date Rates**, **Packets to be sent (per second)**, **Packet Size (bytes)** and **Test Duration (seconds)** drop-down lists..

Step 5 Click **Start**.

Using a Link Test on Mesh Backhaul

Follow the procedure given below to trigger linktest between neighbor mesh APs.

Note Use the **test mesh linktest mac-address** *neighbor-ap-mac* **rate** *data-rate* **fps** *frames-per-second* **frame-size** *frame-size* command to perform link test from an AP.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**ap name** *ap-name* **mesh linktest** *dest-ap-mac data-rate packet-per-sec packet-size test-duration* **Example:** `Device# #ap name ap1 mesh linktest F866.F267.7DFB 24 234 1200 200`	Sets link test parameters.

Configuring Battery State for Mesh AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

Step 2 Choose a profile.

Step 3 In **General** tab, check the **Battery State for an AP** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Battery State for Mesh AP

Some Cisco outdoor APs come with the option of battery backup. There is also a POE-out port that can power a video surveillance camera. The integrated battery can be used for temporary backup power during external power interruptions.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**battery-state** **Example:** `Device(config-wireless-mesh-profile)# battery-state`	Configures the battery state for an AP.

Configuring Mesh Convergence (CLI)

This section provides information about how to configure mesh convergence.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Creates a mesh profile.
Step 3	**convergence {fast | noise-tolerant-fast | standard | very-fast}** **Example:** `Device(config-wireless-mesh-profile)# convergence fast`	Configures mesh convergence method in a mesh profile.

Configuring DHCP Server on Root Access Point (RAP)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP Profile.
Step 3	**dhcp-server** **Example:** `Device(config-ap-profile)# dhcp-server`	Configures DHCP server on the root access point.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Configuring Mesh Ethernet Daisy Chaining (CLI)

The following section provides information about how to configure the Mesh Ethernet Daisy Chaining feature on a mesh AP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile default-ap-profile** **Example:** `Device(config)# ap profile default-ap-profile`	Specifies an AP profile.
Step 3	**ssid broadcast persistent** **Example:** `Device(config-ap-profile)# ssid broadcast persistent`	Configures persistent SSID broadcast and ensures strict wired uplink. RAP will not switch to wireless backhaul when you configure this command.

Enabling Mesh Ethernet Daisy Chaining

The following section provides information about how to enable the Mesh Ethernet Daisy Chaining feature on a Cisco IW 3702 AP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless profile mesh default-mesh-profile** **Example:** `Device(config)# wireless profile mesh default-mesh-profile`	Creates a mesh profile.
Step 3	**ethernet-bridging** **Example:** `Device(config)# ethernet-bridging`	Connects remote wired networks to each other.

	Command or Action	Purpose
Step 4	**no ethernet-vlan-transparent** **Example:** `Device(config)# no ethernet-vlan-transparent`	Disables VLAN transparency to ensure that the bridge is VLAN aware.

Configuring Mesh CAC (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless mesh cac** **Example:** `Device(config)# wireless mesh cac`	Enables mesh CAC mode.

Configuring ATF on Mesh (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Airtime Fairness** > **Global Config**

Step 2 For **5 GHz Band** and **2.4 GHz Band**, enable the **Status** and the **Bridge Client Access** toggle button.

Step 3 To choose the **Mode**, click the **Monitor** or **Enforced** radio button.

Step 4 Enable or disable the **Optimization** toggle button.

Step 5 Enter the **Airtime Allocation**.

Step 6 Click **Apply to Device**.

Configuring ATF on Mesh

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz**} **rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**airtime-fairness bridge-client-access airtime-allocation** *allocation-weight-percentage* **Example:** `Device(config-rf-profile)# airtime-fairness bridge-client-access airtime-allocation 10`	Configures airtime allocation weight percentage on mesh APs.

Create an ATF Policy for a MAP

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**dot11 24ghz airtime-fairness** *atf-policy* **Example:** `Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy`	Enables ATF in the existing RF profile.

Creating an ATF Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Air Time Fairness** > **Profiles**.

Step 2 On the **Profiles** window, click **Add**.

Step 3 In the **Add ATF Policy** window, specify a name, ID, and weight for the ATF policy.

Note Weighted ratio is used instead of percentages so that the total can exceed 100. The minimum weight that you can set is 5.

Step 4 Use the slider to enable or disable the Client Sharing feature.

Step 5 Click **Save & Apply to Device** to save your ATF configuration.

Step 6 (Optional) To delete a policy, check the check box next to the appropriate policy and click **Delete**.

Step 7 (Optional) To edit an existing ATF policy, select the check box next to the policy you want to edit.

In the **Edit ATF Policy** window that is displayed, you can modify the weight and client sharing details for the policy.

Adding an ATF to a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the name of the corresponding policy profile.

Step 3 Click the **Advanced** tab.

Step 4 In the **Air Time Fairness Policies** section, choose the appropriate status for the following: 2.4-GHz Policy and 5-GHz Policy.

Step 5 Click **Update & Apply to Device**.

Enabling ATF Mode in an RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 Click the name of the corresponding RF profile.

Step 3 In the **RF Profile** window, click the **Advanced** tab.

Step 4 In the **ATF Configuration** section, choose the appropriate status for the following:

- **Status**—If you choose **Enabled** as the status, select the **Mode** as either **Monitor** or **Enforced**. Also, you can enable or disable optimization for this mode.
- **Bridge Client Access**
- **Airtime Allocation**—Enter the allocation value. You can set the value only after you enable the **Bridge Client Access**.

Step 5 Click **Update & Apply to Device**.

Enabling Wireless Mesh Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**fast-teardown** **Example:** `Device(config-wireless-profile-mesh)# fast-teardown`	Enables the fast teardown of mesh network and configures the feature's parameter.

Enabling Serial Backhaul in Radio Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio** > **Radio**.

Step 2 Click **Add** to add a radio profile.
The **Add Radio Profile** page is displayed.

Step 3 In the **Add Radio Profile** page, enter the name and description.

Step 4 In the **Mesh Backhaul** field, choose the **Enabled** radio button to enable the feature.

Step 5 In the **Mesh Designated Downlink** field, choose the **Enabled** radio button to enable the feature.

Note Mesh Designated Downlink is supported only on slot number 2 of Mesh APs. You need to be careful while associating radio profiles to the RF tag slots.

Step 6 Click **Apply to Device**.

Enabling Mesh Configurations in Radio Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile radio** *radio-profile-name* **Example:** `Device(config)# wireless profile radio radio-profile-name`	Configures wireless radio profile and goes into radio profile configuration mode.
Step 3	**mesh backhaul** **Example:** `Device(config-wireless-radio-profile)# mesh backhaul`	Enables mesh backhaul. By default, this command is enabled. Mesh backhaul can be disabled on a specific slot, to stop the specific slot from being the backhaul candidate.
Step 4	**mesh designated downlink** **Example:** `Device(config-wireless-radio-profile)# mesh designated downlink`	Enables the radio slot as a designated downlink. By default, this command is disabled. This command is enabled only for slot 2 of the mesh APs. If a slot other than slot 2 is configured as the designated downlink, the following warning message is displayed: `Designated downlink is supported only on slot 2 of mesh APs. Associate in the RF tag accordingly.` By default, all the radio slots are mesh-enabled and not designated as downlink.

Enabling Serial Backhaul (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile radio** *radio-profile-name* **Example:** `Device(config)# wireless profile radio radio-mesh-downlink`	Configures wireless radio profile and goes into radio profile configuration mode.
Step 3	**mesh designated downlink** **Example:** `Device(config-wireless-radio-profile)# mesh designated downlink`	Enables the specified radio as a designated mesh downlink backhaul. Uplink radio will not be used as downlink in the presence of designated downlinks.
Step 4	**exit** **Example:** `Device(config-wireless-radio-profile)# exit`	Exits the submode and returns to global configuration mode.
Step 5	**wireless tag rf** *rf-profile-name* **Example:** `Device(config)# wireless tag rf rf-map-tag`	Configures wireless RF tag and goes into wireless RF tag profile configuration mode. The associate designated downlink is enabled in the radio profile only for slot 2.
Step 6	**dot11 5ghz** {**slot1** | **slot2**} **radio-profile** *radio-profile-name* **Example:** `Device(config-wireless-rf-tag)# dot11 5ghz slot2 radio-profile radio-mesh-downlink`	Configures serial backhaul with the designated downlink radio. **Note** In mesh APs, the uplink and downlink are in the same slot by default. When you configure a designated downlink, the mesh AP is forced to use a specific radio as downlink.

Fallback Mode

Note If at least one radio is configured to be a designated downlink, it means that it will not be used as a potential uplink. To prevent any configuration mistake, for example, configuring uplink radio as the designated downlink, a fallback timer is used in a mesh AP. If the mesh AP is not able to join the controller after the allocated 10 minutes, the designated configurations are cleared and all the radios become uplink-capable.

Configuration Example for Mesh Serial Backhaul

The following example shows how to configure mesh APs with only slot 0 and slot 1 allowed for the mesh AP:

```
Device# configure terminal
Device(config)# wireless profile radio radio-mesh-downlink
Device(config-wireless-radio-profile)# no mesh backhaul
Device(config-wireless-radio-profile)# exit

Device(config)# wireless tag rf rf-map-tag
Device(config-wireless-rf-tag)# dot11 5ghz slot2 radio-profile mesh-disabled
```

Associating Wireless Mesh to an AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile default-ap-profile`	Configures the AP profile and enters AP profile configuration mode.
Step 3	**mesh-profile** *mesh-profile-name* **Example:** `Device(config-ap-profile)# mesh-profile test1`	Configures the mesh profile in AP profile configuration mode.

Configuring Fast Teardown for a Mesh AP Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**.

Step 2 Click **Add**.

Step 3 In the **Add Mesh Profile** window, click **Advanced**.

Step 4 Select a security mode, authentication method, and authorization method.

Step 5 Enable **Ethernet bridging**, if required.

Step 6 Enter the bridge group name and enable Strict Match BGN.

Step 7 Select a band backhaul transmission rate for your radio.

Step 8 Preform the following action in the **Fast Roaming** section:

- Check the **Fast Teardown** check box to detect the root access point uplink failure faster in a mesh deployment and to address fast teardown of the mesh network when an uplink failure occurs.
- In the **Number of Retries** field, enter the number of retries allowed until gateway is considered unreachable. The valid range is between 1 to 10.
- In the **Interval value** field, enter the retry value. The valid range is between 1 to 10 seconds.
- In the **Latency Threshold** field, enter the threshold for a round-trip latency between the AP and the controller. The valid range is between 1 and 500 milliseconds.
- In the **Latency Exceeded Threshold** field, enter the latency interval in which at least one ping must succeed in less than the specified time. The valid range is between 1 to 30 seconds.
- In the **Uplink Recovery Interval** field, enter the time during which root access point uplink must be stable in order to accept the child connections. The valid range is between 1 and 3600 seconds.

Step 9 Click **Apply to Device**.

Configuring Fast Teardown for a Mesh AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh mesh1`	Configures a mesh profile and enters the mesh profile configuration mode.
Step 3	**fast-teardown** **Example:** `Device(config-wireless-mesh-profile)# fast-teardown`	Enables the fast teardown of mesh network and configures the feature's parameter.
Step 4	**enabled** **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# enabled`	Enables the fast teardown feature.
Step 5	**interval** *duration* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# interval 5`	(Optional) Configures the retry interval. The valid values range between 1 and 10 seconds.

	Command or Action	Purpose
Step 6	**latency-exceeded-threshold** *duration* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# latency-exceeded-threshold 20`	(Optional) Specifies the latency interval at which at least one ping must succeed in less than threshold time. The valid values range between 1 and 30 seconds.
Step 7	**latency-threshold** *threshold range* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# latency-threshold 20`	(Optional) Specifies the latency threshold. The valid values range between 1 and 500 milliseconds.
Step 8	**retries** *retry limit* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# retries 1`	(Optional) Specifies the number of retries until the gateway is considered unreachable. The valid values range between 1 and 10.
Step 9	**uplink-recovery-intervals** *recovery interval* **Example:** `Device(config-wireless-mesh-profile-fast-teardown)# uplink-recovery-intervals 1`	(Optional) Specifies the time during which root access point uplink has to be stable to accept child connections. The valid values range between 1 and 3600 seconds.

Flex Resilient with Flex and Bridge Mode Access Points

Information About Flex Resilient with Flex and Bridge Mode Access Points

The Flex Resilient with Flex and Bridge Mode Access Points describe how to set up a controller with Flex+Bridge mode Access Points (APs) and Flex Resilient feature. The Flex Resilient feature works only in Flex+Bridge mode APs. The feature resides in Mesh link formed between RAP - MAP, once the link is UP and RAP loses connection to the CAPWAP controller, both RAP and MAP continue to bridge the traffic. A child Mesh AP (MAP) maintains its link to a parent AP and continues to bridge till the parent link is lost. A child MAP cannot establish a new parent or child link till it reconnects to the CAPWAP controller.

Note Existing wireless clients in locally switching WLAN can stay connected with their AP in this mode. No new or disconnected wireless client can associate to the Mesh AP in this mode. Client traffic in Flex+Bridge MAP is dropped at RAP switchport for the locally switched WLANs.

Configuring a Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click a **Flex Profile Name**. The **Edit Flex Profile** dialog box appears.

Step 3 Under the **General** tab, choose the **Flex Resilient** check box to enable the Flex Resilient feature.

Step 4 Under the **VLAN** tab, choose the required VLANs.

Step 5 (Optionally) Under the **Local Authentication** tab, choose the desired server group from the **Local Accounting RADIUS Server Group** drop-down list. Also, choose the **RADIUS** check box.

Step 6 Click **Update & Apply to Device**.

Configuring a Flex Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex new-flex-profile`	Configures a Flex profile and enters Flex profile configuration mode.
Step 3	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	Enables ARP caching.
Step 4	**description** *description* **Example:** `Device(config-wireless-flex-profile)# description "new flex profile"`	Enables default parameters for the Flex profile.
Step 5	**native-vlan-id** **Example:** `Device(config-wireless-flex-profile)# native-vlan-id 2660`	Configures native vlan-id information.
Step 6	**resilient** **Example:** `Device(config-wireless-flex-profile)# resilient`	Enables the resilient feature.
Step 7	**vlan-name** *vlan_name* **Example:** `Device(config-wireless-flex-profile)# vlan-name VLAN2659`	Configures VLAN name.

	Command or Action	Purpose
Step 8	**vlan-id** *vlan_id* **Example:** `Device(config-wireless-flex-profile)# vlan-id 2659`	Configures VLAN ID. The valid VLAN ID ranges from 1 to 4096.
Step 9	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuring a Site Tag (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site new-flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile new-flex-profile`	Configures a flex profile.
Step 4	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	**Local site** is not configured on the site tag.
Step 5	**site-tag** *site-tag-name* **Example:** `Device(config-site-tag)# site-tag new-flex-site`	Maps a site tag to an AP.
Step 6	**end** **Example:** `Device(config-site-tag)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuring a Mesh Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh Mesh_Profile`	Configures a Mesh profile and enters the Mesh profile configuration mode.
Step 3	**no ethernet-vlan-transparent** **Example:** `Device(config-wireless-profile-mesh)# no ethernet-vlan-transparent`	Disables VLAN transparency to ensure that the bridge is VLAN aware.
Step 4	**end** **Example:** `Device(config-wireless-profile-mesh)# end`	Exits configuration mode and returns to privileged EXEC mode.

Associating Wireless Mesh to an AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile new-ap-join-profile`	Configures the AP profile and enters AP profile configuration mode.
Step 3	**mesh-profile** *mesh-profile-name* **Example:** `Device(config-ap-profile)# mesh-profile Mesh_Profile`	Configures the Mesh profile in AP profile configuration mode.
Step 4	**ssh** **Example:**	Configures the Secure Shell (SSH).

	Command or Action	Purpose
	`Device(config-ap-profile)# ssh`	
Step 5	**mgmtuser username** *username* **password** {**0** | **8**} *password* **Example:** `Device(config-ap-profile)# mgmtuser username Cisco password 0 Cisco secret 0 Cisco`	Specifies the AP management username and password for managing all of the access points configured to the controller. • **0**: Specifies an UNENCRYPTED password. • **8**: Specifies an AES encrypted password. **Note** While configuring an username, ensure that special characters are not used as it results in error with bad configuration.
Step 6	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Attaching Site Tag to an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters ap-tag configuration mode.
Step 3	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag new-flex-site`	Maps a site tag to the AP. **Note** Associating Site Tag causes the associated AP to reconnect.
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuring Switch Interface for APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**interface** *interface-id* **Example:** `Device(config)# interface <int-id>`	Enters the interface to be added to the VLAN.
Step 3	**switchport trunk native vlan** *vlan-id* **Example:** `Device(config-if)# switchport trunk native vlan 2660`	Assigns the allowed VLAN ID to the port when it is in trunking mode.
Step 4	**switchport trunk allowed vlan** *vlan-id* **Example:** `Device(config-if)# switchport trunk allowed vlan 2659,2660`	Assigns the allowed VLAN ID to the port when it is in trunking mode.
Step 5	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Sets the trunking mode to trunk unconditionally. **Note** When the controller works as a host for spanning tree, ensure that you configure portfast trunk, using **spanning-tree portfast trunk** command, in the uplink switch to ensure faster convergence.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying Flex Resilient with Flex and Bridge Mode Access Points Configuration

To view the AP mode and model details, use the following command:

```
Device# show ap name <ap-name> config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-CAP3702I-A-K9
```

To view the MAP mode details, use the following command:

```
Device# show ap name MAP config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-CAP3702I-A-K9
```

To view the RAP mode details, use the following command:

```
Device# show ap name RAP config general | inc AP Mode
AP Mode                                          : Flex+Bridge
AP Model                                         : AIR-AP2702I-A-K9
```

To view if the Flex Profile - Resilient feature is enabled or not, use the following command:

```
Device# show  wireless profile flex detailed FLEX_TAG | inc resilient
Flex resilient                : ENABLED
```

Verifying ATF Configuration on Mesh

You can verify Cisco ATF configurations on mesh APs using the following commands.

Use the following **show** command to display the ATF configuration summary of all the radios:

```
Device# show ap airtime-fairness summary

AP Name                           MAC Address       Slot Admin    Oper        Mode
  Optimization
--------------------------------- ----------------- ---- -------- ----------- --------------
 ------------
ap1/2                            6c:99:89:0c:73:a0 0    ENABLED  DOWN        Enforce-Policy
 Enabled
ap1/2                            6c:99:89:0c:73:a0 1    ENABLED  UP          Enforce-Policy
 Enabled
ap1/3                            6c:99:89:0c:73:a1 0    ENABLED  DOWN        Enforce-Policy
 Enabled
ap1/3                            6c:99:89:0c:73:a1 1    ENABLED  UP          Enforce-Policy
 Enabled
```

Use the following **show** command to display the ATF configuration for a 2.4-GHz radio:

```
Device# show ap dot11 24ghz airtime-fairness

AP Name                           MAC Address       Slot Admin    Oper        Mode
  Optimization
------------------------------- -----------------   ---- -------- ----------- --------------
 ------------
ap1/2                            6c:99:89:0c:73:a0 1    ENABLED  UP          Enforce-Policy
 Enabled
```

Use the following **show** command to display the ATF WLAN statistics:

```
Device# show ap name ap1 dot11 24ghz airtime-fairness wlan 12 statistics

AP Name                           MAC Address       Slot Admin    Oper        Mode
  Optimization
--------------------------------- ----------------- ---- -------- ----------- --------------
 ------------
ap1/2                            6c:99:89:0c:73:a0 0    ENABLED  DOWN        Enforce-Policy
 Enabled
ap1/2                            6c:99:89:0c:73:a0 1    ENABLED  UP          Enforce-Policy
 Enabled      Network level
```

Use the following **show** command to display the wireless mesh summary:

```
Device# show wireless profile mesh summary

Number of Profiles: 2

Profile-Name                      BGN         Security  Bh-access  Description
```

```
-------------------------------------------------------------------------------------------------
mesh1                                           EAP       DISABLED

default-mesh-profile                            EAP       DISABLED   default mesh profile
```

```
Device# show mesh atf client-access

AP Name             Client Access Allocation   Override   Current nodes
                     Default %    Current %
------------------   ---------    ---------    --------   -------------
RAP                     25           40        Enabled          4
RAP                     33           40        Enabled          3
```

Verifying Mesh Ethernet Daisy Chaining

- The following is a sample output of the **show ap config general** command that displays whether a persistent SSID is configured for an AP.

```
Device# show ap 3702-RAP config general

Persistent SSID Broadcast                   Enabled/Disabled
```

- The following is a sample output of the **show wireless mesh persistent-ssid-broadcast summary** command that displays the persistent SSID broadcast status of all the bridge RAPs.

```
Device# show wireless mesh persistent-ssid-broadcast summary

 AP Name     AP Model BVI MAC        BGN        AP Role               Persistent SSID
state
-------     -------- -------       ---       -------             ----------------------
3702-RAP     3702     5c71.0d07.db50 ap_name    Root AP              Enabled
1560-RAP    1562E    380e.4dbf.c6b0 ap_name    Root AP              Disabled
```

Verifying Mesh Convergence

The following is a sample output of the **show wireless profile mesh detailed** command that displays the mesh convergence method used:

```
Device# show wireless profile mesh detailed default-mesh-profile

Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                 : default mesh profile
Convergence Method          : Fast
```

The following is a sample output of the **show wireless mesh convergence subset-channels** command that displays the subset channels of the selected bridge group name:

```
Device# show wireless mesh convergence subset-channels

Bridge group name                Channel
-----------------------------------------
Default                          132
```

Verifying DHCP Server for Root AP Configuration

To verify the DHCP server for root AP configuration, use the following command:

```
Device# show ap config general
Cisco AP Name   : AP4C77.6DF2.D588
================================================
<SNIP>
Dhcp Server                                    : Enabled
```

Verifying Mesh Backhaul

The following is a sample output of the **show ap name mesh backhaul** command that shows details of the mesh backhaul at 2.4 GHz:

```
Device# show ap name test-ap mesh backhaul

MAC Address : xxxx.xxxx.xxxx
Current Backhaul Slot: 0
Radio Type: 0
Radio Subband: All
Mesh Radio Role: DOWNLINK
Administrative State: Enabled
Operation State: Up
Current Tx Power Level:
Current Channel: (11)
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 0
```

The following is a sample output of the **show wireless mesh ap backhaul** command that shows the mesh backhaul details:

```
Device# show wireless mesh ap backhaul

MAC Address : xxxx.xxxx.0x11
Current Backhaul Slot: 1
Radio Type: Main
Radio Subband: All
Mesh Radio Role: Downlink
Administrative State: Enabled
Operation State: Up
Current Tx Power Level: 6
Current Channel: (100)*
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 10
```

The following is a sample output of the **show ap summary** command that shows the radio MAC address and the corresponding AP name:

```
Device# show ap summary
Number of APs: 1
AP Name    Slots  AP Model         Ethernet       MAC Radio MAC  Location         Country
IP Address   State
-----------------------------------------------------------------------------------------------------------------
AP-Cisco-1  2     AIR-APXXXXX-E-K9 xxxx.xxxx.xxd4 xxxx.xxxx.0x11 default location  DE
10.11.70.170 Registered
```

Verifying Mesh Configuration

Use the following **show** commands to verify the various aspects of mesh configuration.

- **show wireless mesh stats** *ap-name*
- **show wireless mesh security-stats** {*all* | *ap-name*}
- **show wireless mesh queue-stats** {*all* | *ap-name*}
- **show wireless mesh per-stats summary** {*all* | *ap-name*}
- **show wireless mesh neighbor summary** {*all* | *ap-name*}
- **show wireless mesh neighbor detail** *ap-name*
- **show wireless mesh ap summary**
- **show wireless mesh ap tree**
- **show wireless mesh ap backhaul**
- **show wireless mesh config**
- **show wireless mesh convergence detail** *bridge-group-name*
- **show wireless mesh convergence subset-channels**
- **show wireless mesh neighbor**
- **show wireless profile mesh detailed** *mesh-profile-name*
- **show wireless stats mesh security**
- **show wireless stats mesh queue**
- **show wireless stats mesh packet error**
- **show wireless mesh ap summary**
- **show ap name** *ap-name* **mesh backhaul**
- **show ap name** *ap-name* **mesh neighbor detail**
- **show ap name** *ap-name* **mesh path**
- **show ap name** *ap-name* **mesh stats packet error**
- **show ap name** *ap-name* **mesh stats queue**
- **show ap name** *ap-name* **mesh stats security**
- **show ap name** *ap-name* **mesh stats**
- **show ap name** *ap-name* **mesh bhrate**
- **show ap name** *ap-name* **config ethernet**
- **show ap name** *ap-name* **cablemodem**
- **show ap name** *ap-name* **environment**

- **show ap name** *ap-name* **gps location**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **mesh linktest data** *dest-mac*
- **show ap environment**
- **show ap gps location**

For details about these commands, see the Cisco Catalyst 9800 Series Wireless Controller Command Reference document.

MAC Authorization

Use the following **show** command to verify the MAC authorization configuration:

```
Device# show run aaa
aaa authentication dot1x CENTRAL_LOCAL local
aaa authorization credential-download CENTRAL_AUTHOR local
username 002cc8de4f31 mac
username 00425a0a53b1 mac

ewlc_eft#sh wireless profile mesh detailed madhu-mesh-profile

Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abbc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
...
Battery State                 : ENABLED
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

PSK Provisioning

Use the following **show** command to verify PSK provisioning configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
```

```
PSK In-use key number                          : 1
Provisioned PSKs(Maximum 5)

Index    Description
------   ------------
1         key1
```

Bridge Group Name

Use the following **show** command to verify the bridge group name configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
Range in feet                 : 12000
Security Mode                 : EAP
Convergence Method            : Fast
LSC only Authentication       : DISABLED
Battery State                 : ENABLED
Authorization Method          : CENTRAL_AUTHOR
Authentication Method         : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Backhaul Client Access

Use the following **show** command to verify the backhaul client access configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
...
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Wireless Backhaul Data Rate

Use the following **show** command to verify the wireless backhaul data rate configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
```

```
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
...
Authorization Method            : CENTRAL_AUTHOR
Authentication Method           : CENTRAL_LOCAL
Backhaul tx rate(802.11bg)      : auto
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

Dynamic Frequency Selection

Use the following **show** command to verify the dynamic frequency selection configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name               : abc-mesh-profile
-------------------------------------------------
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
Amsdu                           : ENABLED
Background Scan                 : ENABLED
Channel Change Notification     : DISABLED
Backhaul client access          : ENABLED
Ethernet Bridging               : ENABLED
Ethernet Vlan Transparent       : DISABLED
Full Sector DFS                 : ENABLED
...
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

Intrusion Detection System

Use the following **show** command to verify the wireless backhaul data rate configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name               : abc-mesh-profile
-------------------------------------------------
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
Amsdu                           : ENABLED
Background Scan                 : ENABLED
Channel Change Notification     : DISABLED
Backhaul client access          : ENABLED
Ethernet Bridging               : ENABLED
Ethernet Vlan Transparent       : DISABLED
Full Sector DFS                 : ENABLED
IDS                             : ENABLED
Multicast Mode                  : In-Out
...
Backhaul tx rate(802.11a)       : 802.11n mcs15
```

Ethernet Bridging

Use the following **show** command to verify ethernet bridging configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name               : abc-mesh-profile
-------------------------------------------------
Description                     :
Bridge Group Name               : bgn-abc
Strict match BGN                : ENABLED
Amsdu                           : ENABLED
Background Scan                 : ENABLED
```

```
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

Multicast over Mesh

Use the following **show** command to verify multicast over Mesh configuration:

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name             : abc-mesh-profile
-------------------------------------------------
Description                   :
Bridge Group Name             : bgn-abc
Strict match BGN              : ENABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : DISABLED
Backhaul client access        : ENABLED
Ethernet Bridging             : ENABLED
Ethernet Vlan Transparent     : DISABLED
Full Sector DFS               : ENABLED
IDS                           : ENABLED
Multicast Mode                : In-Out
...
Backhaul tx rate(802.11a)     : 802.11n mcs15
```

RRM on Mesh Backhaul

Use the following **show** command to verify RRM on Mesh backhaul configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Preferred Parent Selection

Use the following **show** command to verify preferred parent configuration:

```
Device# show wireless mesh ap tree
=========================================================================
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=========================================================================

[Sector 1]
-----------
1542-RAP [0, 0, bgn-madhu, (165), 0000.0000.0000, 1%, 0]
   |-MAP-2700 [1, 67, bgn-madhu, (165), 7070.8b7a.6fb8, 0%, 0]

Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1

(*)  Wait for 3 minutes to update or Ethernet Connected Mesh AP.
(**) Not in this Controller
```

AP Role Change

Use the following **show** command to verify AP role change configuration:

```
Device# show wireless mesh ap summary
AP Name                          AP Model BVI MAC        BGN        AP Role
-------                          -------- -------        ---        -------
1542-RAP                         1542D    002c.c8de.1338 bgn-abc  Root AP
MAP-2700                         2702I    500f.8095.01e4 bgn-abc  Mesh AP

Number of Bridge APs         :   2
Number of RAPs               :   1
Number of MAPs               :   1
Number of Flex+Bridge APs    :   0
Number of Flex+Bridge RAPs   :   0
Number of Flex+Bridge MAPs   :   0
```

Mesh Leaf Node

Use the following **show** command to verify mesh leaf node configuration:

```
Device# show ap name MAP-2700 config general
Cisco AP Name   : MAP-2700
=================================================

Cisco AP Identifier                             : 7070.8bbc.d3e0
Country Code                                    : Multiple Countries : IN,US,IO,J4
Regulatory Domain Allowed by Country            : 802.11bg:-AEJPQU   802.11a:-ABDJNPQU
AP Country Code                                 : IN  - India
AP Regulatory Domain
  Slot 0                                        : -A
  Slot 1                                        : -D
MAC Address                                     : 500f.8095.01e4
...
AP Mode                                         : Bridge
Mesh profile name                               : abc-mesh-profile
AP Role                                         : Mesh AP
Backhaul radio type                             : 802.11a
Backhaul slot id                                : 1
Backhaul tx rate                                : auto
Ethernet Bridging                               : Enabled
Daisy Chaining                                  : Disabled
```

```
Strict Daisy Rap                                : Disabled
Bridge Group Name                               : bgn-abc
Strict-Matching BGN                             : Enabled
Preferred Parent Address                        : 7070.8b7a.6fb8
Block child state                               : Disabled
PSK Key Timestamp                               : Not Configured
...
FIPS status                                     : Disabled
WLANCC status                                   : Disabled
GAS rate limit Admin status                     : Disabled
WPA3 Capability                                 : Disabled
EWC-AP Capability                                : Disabled
AWIPS Capability                                : Disabled
Proxy Hostname                                  : Not Configured
Proxy Port                                      : Not Configured
Proxy NO_PROXY list                             : Not Configured
GRPC server status                              : Disabled
```

Subset Channel Synchronization

Use the following **show** command to verify the subset channel synchronization configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Provisioning LSC for Bridge-Mode and Mesh APs

Use the following **show** command to verify the provisioning LSC for Bridge-Mode and Mesh AP configuration:

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                   : default mesh profile
Bridge Group Name             : bgn-abc
Strict match BGN              : DISABLED
Amsdu                         : ENABLED
Background Scan               : ENABLED
Channel Change Notification   : ENABLED
Backhaul client access        : ENABLED
```

```
Ethernet Bridging             : DISABLED
Ethernet Vlan Transparent     : ENABLED
Full Sector DFS               : ENABLED
IDS                           : DISABLED
Multicast Mode                : In-Out
Range in feet                 : 12000
Security Mode                 : EAP
Convergence Method            : Fast
LSC only Authentication       : DISABLED
Battery State                 : ENABLED
Authorization Method          : default
Authentication Method         : default
Backhaul tx rate(802.11bg)    : auto
Backhaul tx rate(802.11a)     : auto
```

Specify the Backhaul Slot for the Root AP

Use the following **show** command to verify the backhaul slot for the Root AP configuration:

```
Device# show ap name 1542-RAP mesh backhaul
MAC Address : 380e.4d85.5e60
  Current Backhaul Slot: 1
  Radio Type: 0
  Radio Subband: All
  Mesh Radio Role: DOWNLINK
  Administrative State: Enabled
  Operation State: Up
  Current Tx Power Level:
  Current Channel: (165)
  Antenna Type: N/A
  Internal Antenna Gain (in .5 dBm units): 18
```

Using a Link Test on Mesh Backhaul

Use the following **show** command to verify the use of link test on mesh backhaul configuration:

```
Device# show ap name 1542-RAP mesh linktest data 7070.8bbc.d3ef
380e.4d85.5e60 ==> 7070.8bbc.d3ef

Started at : 05/11/2020 20:56:28
Status: In progress

Configuration:
==============
Data rate:  Mbps
Packets per sec: : 234
Packet Size: : 1200
Duration: : 200
```

Mesh CAC

Use the following **show** command to verify mesh CAC configuration:

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                                  : ENABLED
  Mesh CAC                                      : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH)   : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed       : ENABLED
  Rap Channel Sync                              : ENABLED

Mesh Alarm Criteria
  Max Hop Count                                 :  4
```

```
  Recommended Max Children for MAP              : 10
  Recommended Max Children for RAP              : 20
  Low Link SNR                                  : 12
  High Link SNR                                 : 60
  Max Association Number                        : 10
  Parent Change Number                          :  3

Mesh PSK Config
  PSK Provisioning                              : ENABLED
  Default PSK                                   : ENABLED
  PSK In-use key number                         : 1
  Provisioned PSKs(Maximum 5)

  Index    Description
  ------   ------------
  1         key1
```

Verifying Dot11ax Rates on Mesh Backhaul

To verify the 802.11ax rates on mesh backhaul in the mesh profile, use the following command:

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name             : default-mesh-profile
-------------------------------------------------
Description                   : default mesh profile
.
.
Backhaul tx rate(802.11bg)    : 802.11ax mcs7 ss1
Backhaul tx rate(802.11a)     : 802.11ax mcs9 ss2
```

To verify the 802.11ax rates on mesh backhaul in the general configuration of an AP, use the following command:

```
Device# show ap config general
Cisco AP Identifier           : 5c71.0d17.49e0
.
.
Backhaul slot id              : 1
Backhaul tx rate              : 802.11ax mcs7 ss1
```

Verifying Mesh Serial Backhaul

To verify mesh AP serial backhaul, run the following command:

```
Device# show ap name MAP-SB config slot 2 | inc Mesh
Mesh Radio Role : Downlink Access
Mesh Backhaul : Enabled
Mesh Designated Downlink : Enabled
```

To verify serial backhaul enabled on a specific AP, run the following command:

```
Device# show ap name MAP-SB mesh backhaul
MAC Address : 4cxx.4dxx.f4xx
Current Backhaul Slot: 1
Radio Type: Main
Radio Subband: All
Mesh Radio Role: Uplink Access <<<<<<
Administrative State: Enabled
Operation State: Up
```

```
Current Tx Power Level: 6
Current Channel: (104) <<<<<<
Antenna Type:
Internal Antenna Gain (in .5 dBm units): 1
MAC Address : 4cxx.4dxx.f4xx
Current Backhaul Slot: 2
Radio Type: Slave
Radio Subband: All
Mesh Radio Role: Downlink Access <<<<<<
Administrative State: Enabled
Operation State: Up
Current Tx Power Level: 8
Current Channel: (149) <<<<<<
Antenna Type:
Internal Antenna Gain (in .5 dBm units): 1
```

To verify mesh serial backhaul, run the following command:

```
Device# show wireless profile radio detailed radio-mesh-downlink
Radio Profile name                              : radio-mesh-downlink
Description                                     :
Beam-Selection                                  : Not configured
Number of antenna to be enabled                 : 0
Mesh Backhaul                                   : Enabled
Mesh Designated Downlink                        : Enabled
```

Verifying the RRM DCA Status

To view the status of the DCA that is run for mesh APs, run the following command:

```
Device# show ap name Cisco-AP config general | inc Mesh
Mesh profile name                               : default-mesh-profile
Mesh DCA Run Status:                            : Not Running
Last Mesh DCA Run                               : 02/07/2022 01:21:56
```

To verify the status of the last DCA run per radio, run the following command:

```
Device# show wireless mesh rrm dca status
```

Note The output for the **show ap config general | i Mesh** and the **show ap name <AP name> config general | i Mesh** commands, displays only the status for manual RRM DCA triggers that are done via the **ap name <AP name> dot11 rrm channel update mesh** command.

The output for the **show ap config general | i Mesh** and the **show ap name <AP name> config general | i Mesh** commands, does not update if only the global mesh RRM DCA is enabled (auto-dca).

Verifying Fast Teardown with Default Mesh Profile

To verify the fast teardown with the default-mesh-profile, use the following command:

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name            default-mesh-profile
------------------------------------------------------
Fast Teardown                        : ENABLED
Number of Retries                    : 4
Interval in sec                      : 1
```

```
Latency Threshold in msec            : 10
Latency Exceeded Threshold in sec    : 8
Uplink Recovery Interval in sec      : 60
```

Verifying Background Scanning and MAP Fast Ancestor Find

To verify if the Background Scanning and MAP Fast Ancestor Find features are enabled, run the **show wireless profile mesh detailed** command:

```
Device# show wireless profile mesh detailed Mesh_Profile | i Background Scan
Background Scan               : ENABLED
```

```
Device# show wireless profile mesh detailed Mesh_Profile | i MAP fast ancestor find
MAP fast ancestor find        : ENABLED
```

CHAPTER 159

Redundant Root Access Point (RAP) Ethernet Daisy Chaining

- Overview of Redundant RAP Ethernet Daisy Chaining, on page 1747
- Prerequisites for Redundant RAP Ethernet Daisy Chaining Support, on page 1748
- Configuring Redundant RAP Ethernet Daisy Chaining Support (CLI), on page 1748
- Verifying Daisy Chain Redundancy (CLI), on page 1748

Overview of Redundant RAP Ethernet Daisy Chaining

The Root Access Point (RAP) Ethernet Daisy Chaining is a feature where RAPs are chained using wired Ethernet to avoid latency in backhaul link failure recovery.

This feature proposes a redundancy in the daisy chain, wherein, two switches act as a redundant Designated Port (DP), each connected to either end of the daisy chain. In case of a link failure, the link direction is reversed using a new STP root.

A redundant RAP ethernet daisy chain has similiar capabilities to the existing mesh daisy chain feature. In a redundant RAP ethernet daisy chain topology, the packet is encapsulated with CAPWAP header and forwarded to the controller from its wireless client for each AP. The packet is bridged to its primary ethernet interface from its secondary ethernet interface including the other AP's wireless client CAPWAP packets. Both 2.4G and 5G radio are used for client access.

Note The daisy chain strict RAP configuration is applicable to Cisco IOS access points only.

Redundant RAP ethernet daisy chain is supported on the IW6300 AP model.

In case of ethernet daisy chain topology, if a CAPWAP loss occurs on the first RAP connected to switch, the entire chain loses its uplink. This takes a long time to recover. Thereby, if the RAP ethernet daisy chain is enabled, the CAPWAP data keepalive is extended to three times.

Note Only wired uplink configuration is valid, if you configure an AP as Bridge or Flex Bridge mode Root AP.

Prerequisites for Redundant RAP Ethernet Daisy Chaining Support

- Ethernet bridging on should be enabled.
- Strict-wired-uplink feature should be enabled.

Configuring Redundant RAP Ethernet Daisy Chaining Support (CLI)

Follow the procedure given below to enable redundant RAP ethernet daisy chaining on a mesh profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh default-mesh-profile`	Configures a mesh profile and enters mesh profile configuration mode.
Step 3	**daisychain-stp-redundancy** **Example:** `Device(config-wireless-mesh-profile)# daisychain-stp-redundancy`	Configures daisy chain STP redundancy.

Verifying Daisy Chain Redundancy (CLI)

To verify the ethernet daisy chain summary, use the following command:

```
Device# show wireless mesh ethernet daisy-chain summary

AP Name      BVI MAC          BGN     Backhaul      Ethernet         STP Red
-----------------------------------------------------------------------------------------------------
RAP4         683b.78bf.15f0    IOT     Ethernet0     Up  Up  Dn  Dn   Enabled
RAP3         683b.78bf.1634    IOT     Ethernet0     Up  Up  Dn  Dn   Enabled
RAP1         6c8b.d383.b4d4    IOT     Ethernet0     Up  Up  Dn  Dn   Enabled
RAP2         6c8b.d383.b4e8    IOT     Ethernet0     Up  Up  Up  Dn   Enabled
```

To verify the ethernet daisy chain Bridge Group Name (BGN) details, use the following command:

```
Device# show wireless mesh ethernet daisy-chain bgn <IOT>
```

```
AP Name   BVI MAC          BGN    Backhaul    Ethernet          STP Red
-------------------------------------------------------------------------------------------------------
RAP4     683b.78bf.15f0    IOT    Ethernet0   Up  Up  Dn  Dn   Enabled
RAP3     683b.78bf.1634    IOT    Ethernet0   Up  Up  Dn  Dn   Enabled
RAP1     6c8b.d383.b4d4    IOT    Ethernet0   Up  Up  Dn  Dn   Enabled
RAP2     6c8b.d383.b4e8    IOT    Ethernet0   Up  Up  Up  Dn   Enabled
```

To verify the mesh profile, use the following command:

```
Device# show wireless profile mesh detailed default-mesh-profile

Mesh Profile Name : default-mesh-profile
-------------------------------------------------
Description : default mesh profile
Bridge Group Name : IOT
Strict match BGN : ENABLED
Amsdu : ENABLED
Background Scan : ENABLED
Channel Change Notification : ENABLED
Backhaul client access : ENABLED
Ethernet Bridging : ENABLED
Ethernet Vlan Transparent : DISABLED
Daisy Chain STP Redundancy : ENABLED
Full Sector DFS : ENABLED
IDS : ENABLED
Multicast Mode : In-Out
Range in feet : 12000
Security Mode : EAP
Convergence Method : Standard
LSC only Authentication : DISABLED
Battery State : ENABLED
Authorization Method : eap_methods
Authentication Method : eap_methods
Backhaul tx rate(802.11bg) : auto
Backhaul tx rate(802.11a) : auto
===============
```

PART XIV

VideoStream

- VideoStream, on page 1753

CHAPTER 160

VideoStream

- Information about Media Stream, on page 1753
- Prerequisites for Media Stream, on page 1754
- How to Configure Media Stream, on page 1754
- Monitoring Media Streams, on page 1759
- Configuring the General Parameters for a Media Stream (GUI), on page 1760
- Adding Media Stream (CLI), on page 1760
- Enabling a Media Stream per WLAN (GUI), on page 1761
- Enabling a Media Stream per WLAN (CLI), on page 1761
- Configuring the General Parameters for a Media Stream (GUI), on page 1762
- Configuring the General Parameters for a Media Stream (CLI), on page 1762
- Configuring Multicast Direct Admission Control (GUI), on page 1763
- Configuring Multicast Direct Admission Control (CLI), on page 1764
- Create and Attach Policy-based QoS Profile, on page 1765
- Viewing Media Stream Information, on page 1771

Information about Media Stream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable.

The Media Stream feature makes the delivery of the IP multicast stream reliable over air, by converting the multicast frame to a unicast frame over the air. Each Media Stream client acknowledges receiving a video IP multicast stream.

Note Support for IPv6 was added from Cisco IOS XE Gibraltar 16.12.1. You can use IPv6 multicast addresses in place of IPv4 multicast addresses to enable media stream on the IPv6 networks.

Prerequisites for Media Stream

- Make sure that the Multicast feature is enabled. We recommend that you configure IP multicast on the controller in multicast-multicast mode.
- Check for the IP address on the client machine. The machine should have an IP address from the respective VLAN.
- Verify that the access points have joined the controllers .

How to Configure Media Stream

Configuring Multicast-Direct Globally for Media Stream (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** **Example:** `Device(config)# wireless multicast`	Enables multicast for wireless forwarding.
Step 3	**ip igmp snooping** **Example:** `Device(config)# ip igmp snooping`	Enables IGMP snooping on a per-VLAN basis. If the global setting is disabled, then all the VLANs are treated as disabled, whether they are enabled or not.
Step 4	**ip igmp snooping querier** **Example:** `Device(config)# ip igmp snooping querier`	Enables a snooping querier on an interface when there is no multicast router in the VLAN to generate queries.
Step 5	**wireless media-stream multicast-direct** **Example:** `(config)#wireless media-stream multicast-direct`	Configures the global multicast-direct on the controller.

Step 6	**wireless media-stream message**
	Example:
	`(config)#wireless media-stream message ?`
	`  Email  Configure Session Announcement Email`
		Configures various message-configuration parameters such as phone, URL, email, and notes. That is, when a media stream is refused (due to bandwidth constraints), a message can be sent to the corresponding user. These parameters configure the messages that are to

	Command or Action	Purpose
	Notes Configure Session Announcement notes URL Configure Session Announcement URL phone Configure Session Announcement Phone number <cr>	be sent to the IT support email address, notes (message be displayed explaining why the stream was refused), URL to which the user can be redirected, and the phone number that the user can call about the refused stream.
Step 7	**wireless media-stream group** *name startIp endIp* **Example:** (config)#**wireless media-stream group grp1 231.1.1.1 239.1.1.3** avg-packet-size Configure average packet size default Set a command to its defaults exit Exit sub-mode max-bandwidth Configure maximum expected stream bandwidth in Kbps no Negate a command or set its defaults policy Configure media stream admission policy priority Configure media stream priority, <1:Lowest - 8:Highest> qos Configure over the air QoS class, <'video'> ONLY rrc-evaluation Configure RRC re-evaluation admission violation Configure stream violation policy on periodic re-evaluation	Configures each media stream and its parameters such as expected multicast destination addresses, stream bandwidth consumption, and stream-priority parameters.
Step 8	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Media Stream for 802.11 Bands (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream multicast-direct**	Configures whether MediaStream (multicast to unicast) is allowed for the 802.11 band.

	Command or Action	Purpose
	Example: `Device(config)#ap dot11 24ghz media-stream multicast-direct`	You must disable to 802.11 network to enable the MediaStream.
Step 3	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream video-redirect** **Example:** `Device(config)#ap dot11 24ghz media-stream video-redirect`	Optional. Configures the redirection of unicast video traffic to the best-effort queue.
Step 4	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream multicast-direct admission-besteffort** **Example:** `Device(config)#ap dot11 24ghz media-stream multicast-direct admission-besteffort`	Configures the media stream to be sent through the best-effort queue if that media stream cannot be prioritized due to bandwidth-availability limitations. Run the **no** form of the command to drop the stream, if the media stream cannot be prioritized due to bandwidth-availability limitations.
Step 5	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream multicast-direct client-maximum** *value* **Example:** `Device(config)#ap dot11 24ghz media-stream multicast-direct client-max 15`	Configures the maximum number of allowed media streams per individual client. The maximum is 15 and the default is 0. The value of 0 denotes unlimited streams.
Step 6	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream multicast-direct radio-maximum** *value* **Example:** `Device(config)#ap dot11 24ghz media-stream multicast-direct radio-maximum 20`	Configures maximum number of radio streams. The valid range is from 1 to 20. Default is 0. The value of 0 denotes unlimited streams.
Step 7	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac multimedia max-bandwidth** *bandwidth* **Example:** `Device(config)#ap dot11 24ghz cac multimedia max-bandwidth 60`	Configures maximum media (voice + video) bandwidth, in percent. The range is between 5-85%.
Step 8	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac media-stream multicast-direct min-client-rate** *dot11_rate* **Example:** `Device(config)#ap dot11 24ghz cac media-stream multicast-direct min_client_rate`	Configures the minimum PHY rate needed for a client to send a media stream as unicast. Clients communicating below this rate will not receive the media stream as a unicast flow. Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.

	Command or Action	Purpose
Step 9	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac media-stream** **Example:** `Device(config)#ap dot11 5ghz cac media-stream`	Configures Call Admission Control (CAC) parameters for media stream access category.
Step 10	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac multimedia** **Example:** `Device(config)#ap dot11 5ghz cac multimedia`	Configures CAC parameters for media access category: used for voice and video.
Step 11	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac voice** **Example:** `Device(config)#ap dot11 5ghz cac voice`	Configures CAC parameters for voice access category.
Step 12	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a WLAN to Stream Video(GUI)

Procedure

Step 1 Choose **Configuration > Wireless > WLANs > Wireless Networks**.

Step 2 Select a **WLAN** to view the **Edit WLAN** window.

Step 3 Click **Advanced** tab.

Step 4 Check the **Media Stream Multicast-Direct** check box to enable the feature.

Step 5 Click **Update & Apply to Device**.

Configuring a WLAN to Stream Video (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *wlan_name* **Example:** `(config)#wlan wlan50`	Enters WLAN configuration mode.
Step 3	**shutdown** **Example:** `(config-wlan)#shutdown`	Disables the WLAN for configuring its parameters.
Step 4	**media-stream multicast-direct** **Example:** `(config)#media-stream multicast-direct`	Configures the multicast-direct on media stream for the WLAN.
Step 5	**no shutdown** **Example:** `(config-wlan)#no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Deleting a Media Stream (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Media Stream**.

Step 2 Click the **Streams** tab.

Step 3 Check the checkbox adjacent to the Stream Name you want to delete.

To delete multiple streams, select multiple stream name checkboxes.

Step 4 Click **Delete**.

Step 5 Click **Yes** on the confirmation window to delete the VLAN.

Deleting a Media Stream (CLI)

Before you begin

The media stream should be enabled and configured for it to be deleted.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no wireless media-stream group** *media_stream_name* **Example:** `Device(config)#no wireless media-stream grp1`	Deletes the media stream that bears the name mentioned in the command.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Media Streams

Table 127: Commands for monitoring media streams

Commands	Description
show wireless media-stream client detail *group name*	Displays media stream client details of the particular group.
show wireless media-stream client summary	Displays the media stream information of all the clients.
show wireless media-stream group detail *group name*	Displays the media stream configuration details of the particular group.
show wireless media-stream group summary	Displays the media stream configuration details of all the groups.
show wireless media-stream message details	Displays the session announcement message details.
show wireless multicast	Displays the multicast-direct configuration state.
show ap dot11 {24ghz | 5ghz} media-stream rrc	Displays 802.11 media Resource-Reservation-Control configurations.

Configuring the General Parameters for a Media Stream (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Media Stream**.

Step 2 In the **General** tab, check the **Multicast Direct Enable** check box.

Step 3 In the **Session Message Config** section, check the **Session Announcement State** check box to enable the session announcement mechanism. If the session announcement state is enabled, clients are informed each time a controller is not able to serve the multicast direct data to the client.

Step 4 In the **Session Announcement URL** field, enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.

Step 5 In the **Session Announcement Email** field, enter the e-mail address of the person who can be contacted.

Step 6 In the **Session Announcement Phone** field, enter the phone number of the person who can be contacted.

Step 7 In the **Session Announcement Note** field, enter a reason as to why a particular client cannot be served with a multicast media.

Step 8 Click **Apply**.

Adding Media Stream (CLI)

Procedure

	Command or Action	Purpose
Step 1	**wireless media-stream group** *groupName startIpAddr endIpAddr* **Example:** `Device(config)# wireless media-stream group group1 224.0.0.0 224.0.0.223`	Configures each media stream and its parameters, such as expected multicast destination addresses, stream bandwidth consumption , and stream priority parameters.
Step 2	**avg-packet-size** *packetsize* **Example:** `Device(media-stream)# avg-packet-size 100`	Configures the average packet size.
Step 3	**max-bandwidth** *bandwidth* **Example:** `Device(media-stream)# max-bandwidth 80`	Configures the maximum expected stream bandwidth, in Kbps.
Step 4	**policy** { **admit** | **deny** } **Example:** `Device(media-stream)# policy admit`	Configure the media stream admission policy.

	Command or Action	Purpose
Step 5	**qos video** **Example:** `Device(media-stream)# qos video`	Configures over-the-air QoS class, as 'video'.
Step 6	**violation** { **drop** | **fallback** } **Example:** `Device(media-stream)# violation drop`	Configures the violation mode.
Step 7	**rrc-evaluation** { **initial** | **periodic** } **Example:** `Device(media-stream)# rrc-evaluation initial`	Configure Resource Reservation Control (RRC) re-evaluation admission, which provides initial or periodic admission evaluation. The re-evaluation admission occurs at 2, 4,8, and so on seconds.
Step 8	**priority** *priority-value* **Example:** `Device(media-stream)# priority 6`	Sets the priority value. The valid range is from 1-8, with 1 being the lowest.

Enabling a Media Stream per WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.
Step 2 On the **WLANs** page, click the name of the **WLAN** or click **Add** to create a new one.
Step 3 In the **Add/Edit WLAN** window that is displayed, click the **Advanced** tab.
Step 4 Check the **Enabling a Media Stream for each WLAN** check box to enable Media Stream on the WLAN.
Step 5 Save the configuration.

Enabling a Media Stream per WLAN (CLI)

Follow the procedure given below to enable a media stream for each WLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *wlan_name* **Example:** `Device(config)# wlan wlan5`	Enters WLAN configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN for configuring its parameters.
Step 4	**media-stream multicast-direct** **Example:** `Device(config-wlan)# media-stream multicast-direct`	Configures multicast-direct for the WLAN.
Step 5	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring the General Parameters for a Media Stream (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Media Stream**.

Step 2 Check the **Multicast Direct Enable** check box to enable multicast direct globally on the local mode.

Step 3 In the **Session Message Config** section, enter the values for the following parameters

- Session Announcement URL
- Session Announcement Email
- Session Announcement Phone
- Session Announcement Note

Step 4 Save the configuration.

Configuring the General Parameters for a Media Stream (CLI)

Follow the procedure given below to configure the general parameters for a media stream:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless media-stream message** { **URL** *url* | **email** *email-address* | **phone** *phone-no* | **notes** *notes* } **Example:** `Device(config)# wireless media-stream message url www.xyz.com`	Configures various message configuration parameters, such as phone, URL, email, and notes.
Step 3	**wireless media-stream multicast-direct** **Example:** `Device(config)# wireless media-stream multicast-direct`	Enables multicast direct globally for local mode. **Note** This configuration will not impact flex and fabric media-stream configurations.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuring Multicast Direct Admission Control (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Media Stream**.

Step 2 Check the **Media Stream Admission Control (ACM)** check box to enable multicast direct admission control.

Step 3 In the **Maximum Media Stream RF bandwidth (%)** field, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Valid range is from 5 to 85. When the client reaches a specified value, the AP rejects new calls on this radio band.

Step 4 In the **Maximum Media Bandwidth (%)** field, enter the bandwidth. Valid range is from 5 to 85%.

Step 5 From the **Client Minimum Phy Rate** drop-down list, select the minimum transmission data rate or the rate in kilobits per second at which the client can operate. If the transmission data rate is below the physical rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

Step 6 In the **Maximum Retry Percent (%)** field, enter the percentage of maximum retries that are allowed. The default value is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

Step 7 Click **Apply**.

Configuring Multicast Direct Admission Control (CLI)

Follow the procedure given below to configure multicast direct admission control:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **shutdown** **Example:** `Device(config)# ap dot11 24ghz shutdown`	Disables the 802.11 network.
Step 3	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream video-redirect** **Example:** `Device(config)# ap dot11 24ghz media-stream video-redirect`	Configures the redirection of the unicast video traffic to best-effort queue.
Step 4	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac media-stream acm** **Example:** `Device(config)# ap dot11 24ghz cac media-stream acm`	Enables admission control on the media-stream access category.
Step 5	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac media-stream max-bandwidth** *bandwidth* **Example:** `Device(config)# ap dot11 24ghz cac media-stream max-bandwidth 65`	Configures the maximum media bandwidth, in percent. The range is between 5-85%.
Step 6	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac multimedia max-bandwidth** *bandwidth* **Example:** `Device(config)# ap dot11 24ghz cac multimedia max-bandwidth 65`	Configures the maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for media. The range is between 5-85%.
Step 7	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac media-stream multicast-direct min-client-rate** *dot11Rate* **Example:** `Device(config)# ap dot11 24ghz cac media-stream multicast-direct min-client-rate 800`	Configures the minimum PHY rate needed for a client to receive media stream as unicast. Clients communicating below this rate will not receive the media stream as a unicast flow. Typically, this PHY rate is equal to or higher than the rate at which multicast frames are sent.

	Command or Action	Purpose
Step 8	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cac media-stream multicast-direct max-retry-percent** *retryPercent* **Example:** `Device(config)# ap dot11 24ghz cac media-stream multicast-direct max-retry-percent 50`	Configures CAC parameter maximum retry percent for multicast-direct streams.
Step 9	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream multicast-direct radio-maximum** *value* **Example:** `Device(config)# ap dot11 24ghz media-stream multicast-direct radio-maximum 10`	Configures the maximum number of radio streams. The range is from 1 to 20. Default is 0. Value 0 denotes unlimited streams.
Step 10	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream multicast-direct client-maximum** *value* **Example:** `Device(config)# ap dot11 24ghz media-stream multicast-direct client-maximum 12`	Configures the maximum number of allowed media streams per individual client. The maximum is 15 and the default is 0. Value 0 denotes unlimited streams.
Step 11	**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **media-stream multicast-direct admission-besteffort** **Example:** `Device(config)# ap dot11 24ghz media-stream multicast-direct admission-besteffort`	Configures the media stream to still be sent through the best effort queue if a media stream cannot be prioritized due to bandwidth availability limitations. Add **no** in the command to drop the stream if the media stream cannot be prioritized due to bandwidth availability limitations.
Step 12	**no ap dot11** {**24ghz** | **5ghz** | **6ghz**} **shutdown** **Example:** `Device(config)# no ap dot11 24ghz shutdown`	Enables the 802.11 network.

Create and Attach Policy-based QoS Profile

The high-level steps to create and attach policy-based QoS profile are as follows:

1. Create a QoS Profile
2. Create a Service Template
3. Map the Service Template to the Policy Map
4. Map the Policy Map to the Policy Profile

Create a QoS Profile (GUI)

Procedure

Step 1 Click **Configuration** > **Services** > **QoS**.

Step 2 Click **Add** to create a new QoS Policy.

Step 3 Enter a **Policy Name**.

Step 4 Enter a **Description** for the policy.

Step 5 In the **Class Default** section, choose a value in the **Mark** drop-down list.

Step 6 Enter the **Police(kbps)** value.

Step 7 Click **Apply to Device**.

Create a QoS Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map QoS_Drop_Youtube`	Creates a policy map.
Step 3	**description** *description* **Example:** `Device(config-pmap)# description QoS_Drop_Youtube`	Adds a description to the policy map.
Step 4	**class** *class-map-name* **Example:** `Device(config-pmap)# class QoS_Drop_Youtube1_AVC_UI_CLASS`	Creates a policy criteria.
Step 5	**police cir** *committ-information-rate* **Example:** `Device(config-pmap-c)# police cir 8000`	Polices the provided committed information rate.
Step 6	**conform-action drop** **Example:**	Configures the action when the rate is less than the conform burst.

	Command or Action	Purpose
	`Device(config-pmap-c-police)# conform-action drop`	
Step 7	**exceed-action drop** **Example:** `Device(config-pmap-c-police)# exceed-action drop`	Configures the action when the rate is within the conform and conform plus exceed burst.
Step 8	**end** **Example:** `Device(config-pmap-c-police)# end`	Returns to privileged EXEC mode.

Create a Service Template (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policy**.

Step 2 On the **Local Policy** page, **Service Template** tab, click **Add**.

Step 3 In the **Create Service Template** window, enter the following parameters:

- **Service Template Name:** Enter a name for the template.
- **VLAN ID:** Enter the VLAN ID for the template. Valid range is between 1 and 4094.
- **Session Timeout (secs):** Sets the timeout duration for the template. Valid range is between 1 and 65535.
- **Access Control List:** Choose the Access Control List from the drop-down list.
- **Ingress QOS:** Choose the input QoS policy for the client from the drop-down list
- **Egress QOS:** Choose the output QoS policy for the client from the drop-down list.

Step 4 Click **Apply to Device**.

Create a Service Template (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**service-template** *template-name* **Example:** `Device(config)# service-template qos-template`	Configures the service-template or identity policy.
Step 3	**vlan** *vlan-id* **Example:** `Device(config-service-template)# vlan 87`	Specifies VLAN ID.
Step 4	**absolute-timer** *timer* **Example:** `Device(config-service-template)# absolute-timer 3600`	Specifies session timeout value for a service template.
Step 5	**service-policy qos input** *qos-policy* **Example:** `Device(config-service-template)# service-policy qos input QoS_Drop_Youtube`	Configures an input QoS policy for the client.
Step 6	**service-policy qos output** *qos-policy* **Example:** `Device(config-service-template)# service-policy qos output QoS_Drop_Youtube`	Configures an output QoS policy for the client.
Step 7	**end** **Example:** `Device(config-service-template)# end`	Returns to privileged EXEC mode.

Map the Service Template to the Policy Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, select the **Policy Profile** to be mapped.

Step 3 In the **Edit Policy Profile** window, click **Access Policies** tab.

Step 4 Use the **Local Subscriber Policy Name** drop-down list to select the policy name.

Step 5 Click **Update & Apply to Device**.

Map the Service Template to the Policy Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Device(config)# parameter-map type subscriber attribute-to-service QoS-Policy_Map-param`	Specifies the parameter map type and name.
Step 3	*map-index* **map device-type eq** *filter-name* **user-role eq** *user-name* **Example:** `Device(config-parameter-map-filter)# 1 map device-type eq "Android" user-role eq "student"`	Specifies the parameter map attribute filter criteria. Multiple filters are used in the example provided here.
Step 4	*map-index* **service-template** *service-template-name* **precedence** *precedence-num* **Example:** `Device(config-parameter-map-filter-submode)# 1 service-template Qos_template`	Specifies the service template.
Step 5	**end** **Example:** `Device(config-parameter-map-filter-submode)# end`	Returns to privileged EXEC mode.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 7	**policy-map type control subscriber** *policy-map-name* **Example:** `Device(config)# policy-map type control subscriber QoS-Policy_Map`	Specifies the policy map type.
Step 8	**event identity-update match-all** **Example:**	Specifies the match criteria to the policy map.

	Command or Action	Purpose
	`Device(config-event-control-policymap)# event identity-update match-all`	
Step 9	*class-num* **class always do-until-failure** **Example:** `Device(config-event-control-policymap)# 1 class always do-until-failure`	Applies a class-map with a service-template.
Step 10	*action-index* **map attribute-to-service table** *parameter-map-name* **Example:** `Device(config-event-control-policymap)# 1 map attribute-to-service table QoS-Policy_Map-param`	Applies a parameter map.

Map the Policy Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local Policy** > **Policy Map** tab.
Step 2 Click **Add**.
Step 3 Enter a name in the **Policy Map Name** text field.
Step 4 Click **Add** to add the matching criteria information.
Step 5 Choose the service template from the **Service Template** drop-down list.
Step 6 Choose the filters from **Device Type**, **User Role**, **User Name**, **OUI** and **MAC Address** drop-down lists.
Step 7 Click **Add Criteria**
Step 8 Click **Apply to Device**.

Map the Policy Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:**	Configures a wireless policy profile.

	Command or Action	Purpose
	`Device(config)# wireless profile policy test-policy-profile`	
Step 3	**description** *profile-policy-description* **Example:** `Device(config-wireless-policy)# description "test policy profile"`	Adds a description for the policy profile.
Step 4	**subscriber-policy-name** *policy-name* **Example:** `Device(config-wireless-policy)# subscriber-policy-name QoS-Policy_Map`	Configures the subscriber policy name.

Viewing Media Stream Information

Use the following **show** commands to view the media stream information.

To view media stream general information and status, use the following commands:

```
Device# show wireless media-stream multicast-direct state

Multicast-direct State........................... : enabled
Allowed WLANs:
WLAN-Name                                          WLAN-ID
-----------------------------------------------------------
zsetup_mc                                          1
vwlc-mc_mo                                         3
mcuc_test1                                         4
mcuc_test2                                         5


Device# show wireless media-stream group summary


Number of Groups:: 4

Stream Name          Start IP                End IP            Status
-------------------------------------------------------------------------------
new2                 231.2.2.3               231.2.4.4         Enabled
my234                234.0.0.0               234.10.10.10      Enabled
uttest2              235.1.1.20              235.1.1.25        Enabled
uttest3              235.1.1.40              235.1.1.200       Enabled
```

To view the details of a particular media stream, use the **show wireless media-stream client detail** *media_stream_name* command:

```
Device# show wireless media-stream group detail uttest2


Media Stream Name         : uttest2
Start IP Address          : 235.1.1.20
End IP Address            : 235.1.1.25
RRC Parameters:
 Avg Packet Size(Bytes)   : 1200
 Expected Bandwidth(Kbps) : 1000
```

```
 Policy                   : Admitted
 RRC re-evaluation        : Initial
 QoS                      : video
 Status                   : Multicast-direct
 Usage Priority           : 4
 Violation                : Drop
```

To view RRC information for a dot11 band, use the **show ap dot11** {**24ghz | 5ghz | 6ghz**} **mediastream rrc** command:

```
Device# show  ap dot11 5ghz media-stream rrc

Multicast-direct                : Enabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio   : Auto
Max Allowed Streams Per Client  : 5
Max Media-Stream Bandwidth      : 5
Max Voice Bandwidth             : 50
Max Media Bandwidth             : 43
Min PHY Rate (Kbps)             : 6000
Max Retry Percentage            : 5
```

To view session announcement message details, use the **show wireless media-stream message details** command:

```
Device# show wireless media-stream message details
URL          :
Email        : abc@cisc
Phone        :
Note         :
State        : Disabled
```

To view the list of clients in the blocked list database, use the **show ip igmp snooping igmpv2-tracking** command:

```
Device# show ip igmp snooping igmpv2-tracking

Client to SGV mappings
----------------------
Client: 10.10.10.215 Port: Ca1
 Group: 239.255.255.250 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.7 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.8 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.9 Vlan: 10 Source: 0.0.0.0 blacklisted: no

Client: 10.10.101.177 Port: Ca2
 Group: 235.1.1.14 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 235.1.1.16 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 235.1.1.18 Vlan: 10 Source: 0.0.0.0 blacklisted: no

SGV to Client mappings
----------------------
Group: 234.5.6.7 Source: 0.0.0.0 Vlan: 10
 Client: 10.10.10.215 Port: Ca1 Blacklisted: no
```

To view wireless client summary, use the **show wireless media-stream client summary** command:

```
Device# show wireless media-stream client summary
```

To view details of a specific wireless media stream, use the **show wireless media-stream client detail** command:

```
Device# show wireless media-stream client detail uttest2

Media Stream Name         : uttest2
Start IP Address          : 235.1.1.20
End IP Address            : 235.1.1.25
RRC Parameters:
 Avg Packet Size(Bytes)   : 1200
 Expected Bandwidth(Kbps) : 1000
 Policy                   : Admitted
 RRC re-evaluation        : Initial
 QoS                      : video
 Status                   : Multicast-direct
 Usage Priority           : 4
 Violation                : Drop
```

PART XV

Software-Defined Access Wireless

- Software-Defined Access Wireless, on page 1777
- Passive Client, on page 1789
- Fabric in a Box with External Fabric Edge, on page 1797

CHAPTER 161

Software-Defined Access Wireless

- Information to Software-Defined Access Wireless, on page 1777
- Information About SD-Access Wireless Mesh Inter Fabric Edge Switch Roaming Protection, on page 1780
- Configuring SD-Access Wireless, on page 1782
- Verifying SD-Access Wireless, on page 1786

Information to Software-Defined Access Wireless

The Enterprise Fabric provides end-to-end enterprise-wide segmentation, flexible subnet addressing, and controller-based networking with uniform enterprise-wide policy and mobility. It moves the enterprise network from current VLAN-centric architecture to a user group-based enterprise architecture, with flexible Layer 2 extensions within and across sites.

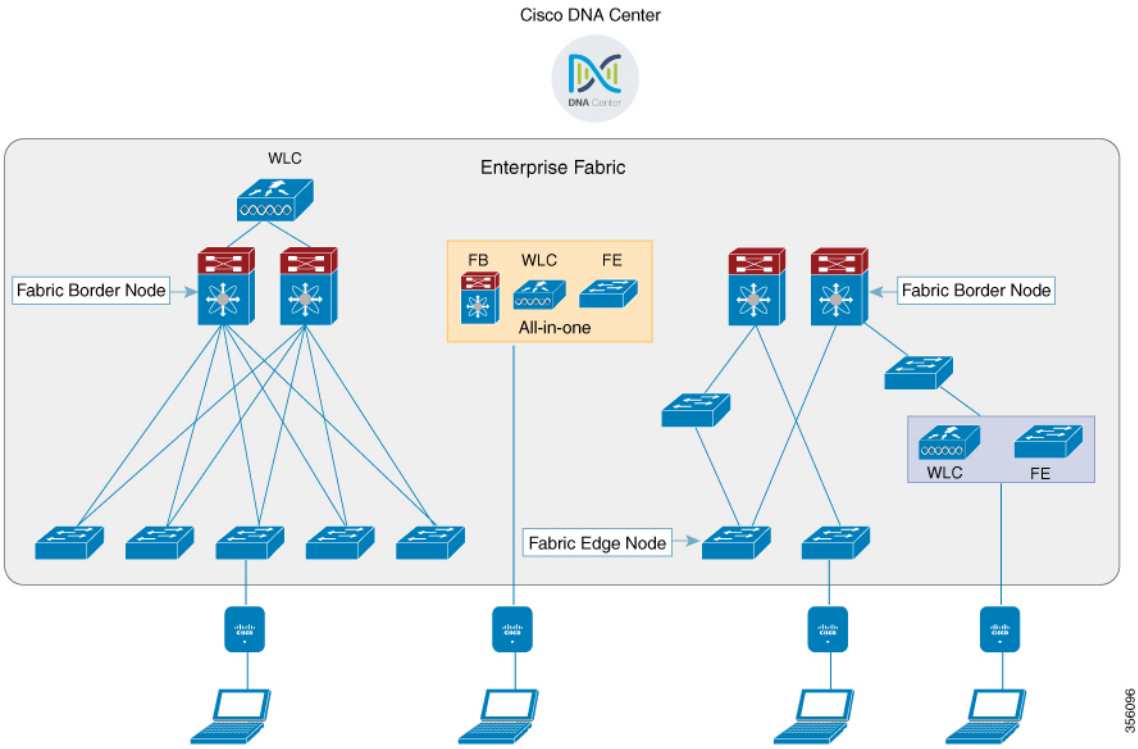
Enterprise fabric is a network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device. This provides seamless connectivity, with policy application and enforcement at the edge of the fabric. Fabric uses IP overlay, which makes the network appear as a single virtual entity without using clustering technologies.

The following definitions are used for fabric nodes:

- **Enterprise Fabric**: A network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device.
- **Fabric Domain**: An independent operation part of the network. It is administered independent of other fabric domains.
- **End Points**: Hosts or devices that connect to the fabric edge node are known as end points (EPs). They directly connect to the fabric edge node or through a Layer 2 network.

The following figure shows the components of a typical SD-Access Wireless. It consists of Fabric Border Nodes (BN), Fabric Edge Nodes (EN), Wireless Controller, Cisco Catalyst Center, and Host Tracking Database (HDB).

Figure 51: Software-Defined Access Wireless



The figure covers the following deployment topologies:

- All-in-one Fabric—When we have all Fabric Edge, Fabric Border, Control-Plane and controller functionality enabled on a Cat 9K switch.

  This topology is depicted in the mid part of the figure.

- Split topology—When we have Fabric Border, or Control Plane, or controller on a Cat 9K switch with separate Fabric Edge. This topology is depicted in the left-most part of the figure.

- Co-located Fabric Edge and Controller—When we have Fabric Edge and controller on a Cat 9K switch. This topology is depicted in the right-most part of the figure.

Cisco Catalyst Center: Is an open, software-driven architecture built on a set of design principles with the objective of configuring and managing Cisco Catalyst 9800 Series Wireless Controllers.

Control Plane: This database allows the network to determine the location of a device or user. When the EP ID of a host is learnt, other end points can query the database about the location of the host. The flexibility of tracking subnets helps in summarization across domains and improves the scalability of the database.

Fabric Border Node (Proxy Egress Tunnel Router [PxTR or PITR/PETR] in LISP): These nodes connect traditional Layer 3 networks or different fabric domains to the enterprise fabric domain. If there are multiple fabric domains, these nodes connect a fabric domain to one or more fabric domains, which could be of the same or different type. These nodes are responsible for translation of context from one fabric domain to another. When the encapsulation is the same across different fabric domains, the translation of fabric context is generally 1:1. The fabric control planes of two domains exchange reachability and policy information through this device.

Fabric Edge Nodes (Egress Tunnel Router [ETR] or Ingress Tunnel Router [ITR] in LISP): These nodes are responsible for admitting, encapsulating or decapsulating, and forwarding of traffic from the EPs. They lie at the perimeter of the fabric and are the first points of attachment of the policy. EPs could be directly or indirectly attached to a fabric edge node using an intermediate Layer 2 network that lies outside the fabric domain. Traditional Layer 2 networks, wireless access points, or end hosts are connected to fabric edge nodes.

Wireless Controller: The controller provides AP image and configuration management, client session management and mobility. Additionally, it registers the mac address of wireless clients in the host tracking database at the time of client join, as well as updates the location at the time of client roam.

Access Points: AP applies all the wireless media specific features. For example, radio and SSID policies, webauth punt, peer-to-peer blocking, and so on. It establishes CAPWAP control and data tunnel to controller. It converts 802.11 data traffic from wireless clients to 802.3 and sends it to the access switch with VXLAN encapsulation.

The SDA allows to simplify:

- Addressing in wireless networks
- Mobility in wireless networks
- Guest access and move towards multi-tenancy
- Leverage Sub-net extension (stretched subnet) in wireless network
- Provide consistent wireless policies

Note Role co-location between wireless controller and fabric edge is supported.

Platform Support

Table 128: Supported Platforms for Software-Defined Access Wireless

Platforms	Support
Catalyst 9300	Yes
Catalyst 9400	Yes
Catalyst 9500H	Yes
Cisco Catalyst 9800 Series Wireless Controller for Cloud	Yes
Cisco Catalyst 9800-40 Series Wireless Controller	Yes
Cisco Catalyst 9800-80 Series Wireless Controller	Yes

Table 129: Multi-Instance Support

Multi-instance	Support
Multiple LISP sessions	Yes

Multi-instance	Support
Emulated database support	Yes
Client roaming between WNCd instances	Yes

Table 130: Feature Support

Feature	Support
Inter-WLC roam for IRCM	Only L2 mobility is supported as VLAN is stretched across the fabric.
DNS-IPv4-ACL	• ACLs are enforced at AP. • Controller needs to push the DNS-ACL information to AP.
IPv6 ACL for clients	Yes. Open, 802.11x, WebAuth, PSK WLANs, IPv6 address visibility are also supported.
Location tracking/Hyperlocation	Yes
Multicast Video-Stream (IPv4)	Yes
Smart Licensing	Yes

Table 131: Outdoor Access Points Support

AP	Support
1542	Yes
1560	Yes

Information About SD-Access Wireless Mesh Inter Fabric Edge Switch Roaming Protection

When a Mesh AP (MAP) finds a Root AP (RAP) or other MAP with better adjacency, it roams to that RAP or MAP. However, a MAP cannot roam to another MAP or RAP connected to a different fabric edge switch due to wireless client connectivity loss. The reason being the VXLAN tunnels of the wireless client cannot be moved to another fabric edge switch.

However, if the current MAP link is much worse than the link to RAP or MAP connected to a different fabric edge switch, then the MAP roams and restart its CAPWAP tunnel.

Thus, all the MAPs connected to the MAP restarts the CAPWAP tunnels as well. This allows the wireless clients to connect again and creates wireless client VXLAN tunnels in the fabric edge.

Note The criteria for a MAP roaming to a RAP or MAP connected to a different fabric edge switch are the same as the mesh preferred parent. They are:

- If the current link SNR is worse than 12 dB and there is another better link. (Or)
- If the current link SNR is worse than 20 dB and there is another link with 20% or better SNR.

The mesh daisy chain roaming is not supported in RAP or MAP connected to different fabric edge switches.

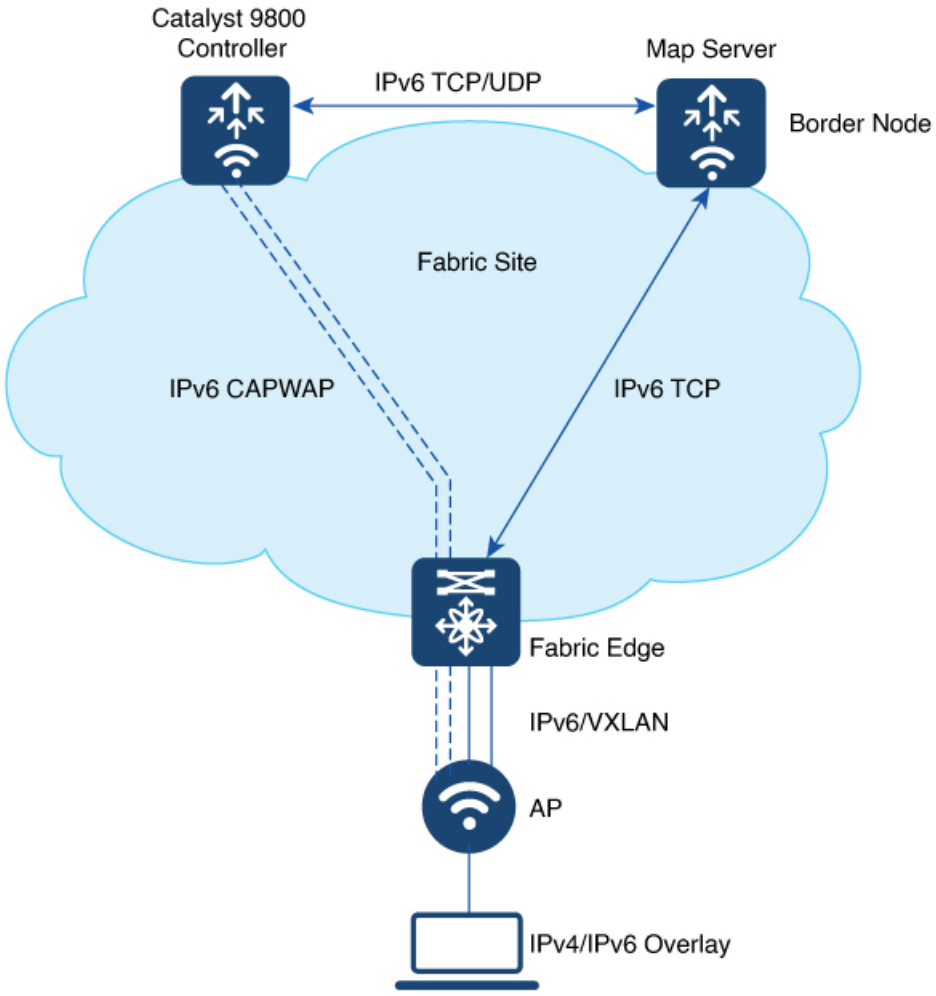
SDA IPv6 Underlay Support

This feature provides a wireless SDA IPv6 underlay support to enable IPv6-based communications in a fabric site. IPv6 is used to establish LISP connections between the controller and map server as well as between the map server and Fabric Edge. IPv6 underlay is also used to construct a VXLAN tunnel between the Fabric Edge and the AP.

The feature implementation is as follows:

- **Catalyst 9800 Controller**:
  - The controller manages IPv6-based LISP sessions to the map server
  - Encodes, decodes, and processes LISP messages through IPv6 TCP/UDP sockets.)
  - Communicates RLOC IPv6 address to the AP for VXLAN creation and client tunnel mapping
- **Fabric Edge**:
  - Processes map notification from map server
  - Creates IPv6 VXLAN tunnel
  - Maps client to IPv6 VXLAN tunnel
  - Encapsulates and decapsulates client traffic into and out of VXLAN tunnel
- **Access Points**:
  - Processes fabric TLV from the controller
  - Creates IPv6 VXLAN tunnel
  - Encapsulates and decapsulates client traffic into and out of VXLAN tunnel

The following figure shows the feature architecture:



Note For AP to join controller using IPv6 address, ensure that you configure the preferred mode in AP profile as IPv6.

Restrictions

Embedded wireless controller (EWC) on Catalyst 9k switches is not supported.

Configuring SD-Access Wireless

- To enable SD-Access wireless globally, you need to run the **wireless fabric** configuration command.
- During SD-Access Wireless provisioning, ensure that L2-VNID value is unique.

Configuring Default Map Server (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless Plus** > **Fabric** > **Fabric Configuration**.

Step 2 In the **Map Server** section, specify the IP address and preshared key details for Server 1.

Step 3 Optionally, you can specify the IP address and preshared key details for Server 2.

Step 4 Click **Apply**.

Configuring Default Map Server (CLI)

Follow the procedure given below to configure default map server:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless fabric control-plane** *map-server-name* **Example:** `Device(config)# wireless fabric control-plane map-server-name`	Configures the default map server. Here, *map-server-name* defines a pair of map servers.
Step 3	**ip address** *ip-address* **key** *user_password reenter_password* **Example:** `Device(config-wireless-cp)# ip address 200.0.0.0 key user-password user-password`	Configures IP address for the default map server.
Step 4	**end** **Example:** `Device(config-wireless-cp)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring SD-Access Wireless Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Fabric**.

Step 2 On the **Fabric** page, click the **Profiles** tab and click **Add**.

Step 3 In the **Add New Profile** window that is displayed, specify the following parameters:

- Profile name
- Description
- L2 VNID; valid range is between 0 and 16777215
- SGT tag; valid range is between 2 and 65519

Step 4 Click **Save & Apply to Device**.

Configuring SD-Access Wireless Profile (CLI)

Follow the procedure given below to configure SD-Access wireless profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless profile fabric** *fabric-profile-name* **Example:** `Device(config)# wireless profile fabric fabric-profile-name`	Configures the SD-Access wireless profile parameters.
Step 3	**sgt-tag** *sgt* **Example:** `Device(config-wireless-fabric)# sgt-tag 2`	Configures SGT tag. Here, *sgt* refers to the sgt tag value. The valid range is from 2-65519. The default value is 0.
Step 4	**client-l2-vnid** *client-l2-vnid* **Example:** `Device(config-wireless-fabric)# client-l2-vnid client-l2-vnid`	Configures client L2-VNID. Here, *client-l2-vnid* refers to the client L2-VNID value. The valid range is from 0-16777215.
Step 5	**end** **Example:** `Device(config-wireless-fabric)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Map Server in Site Tag (GUI)

Before you begin

Ensure that you have configured a control plane at the time of configuring Wireless Fabric.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page, click the **Site** tab.

Step 3 Click the name of the site tag.

Step 4 In the **Edit Site Tag** window, choose the Fabric control plane name from the **Control Plane Name** drop-down list.

Step 5 Save the configuration.

Configuring Map Server in Site Tag (CLI)

Follow the procedure given below to configure map server in site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless tag site** *site-tag* **Example:** `Device(config)# wireless tag site default-site-tag`	Configures site tag. Here, *site-tag* refers to the site tag name.
Step 3	**fabric control-plane** *map-server-name* **Example:** `Device(config-site-tag)# fabric control-plane map-server-name`	Configures fabric control plane details. Here, *map-server-name* refers to the fabric control plane name associated with the site tag.
Step 4	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Map Server per L2-VNID (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Fabric**.

Step 2 On the **Fabric Configuration** page in the **Fabric VNID Mapping** section, click **Add**.

Step 3 In the **Add Client and AP VNID** window, specify a name for the Fabric, L2 VNID value (valid range is from 0 to 4294967295), control plane name.

Step 4 Save the configuration.

Configuring Map Server per L2-VNID (CLI)

Follow the procedure given below to configure map server in site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless fabric name** *name* **l2-vnid** *l2-vnid-value* **l3-vnid** *l3-vnid-value* **ip** *network-ip subnet-mask* **control-plane-name** *control-plane-name* **Example:** `Device(config)# wireless fabric name fabric_name l2-vnid 2 l3-vnid 2 ip 122.220.234.0 255.255.0.0 control-plane-name sample-control-plane`	Configures the map server to the VNID map table. • *name* refers to the fabric name. • *l2-vnid-value* refers to the L2 VNID value. The valid range is from 0 to 16777215. • *L3-vnid-value* refers to the L3 VNID value. The valid range is from 0 to 16777215. • *control-plane-name* refers to the control plane name.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying SD-Access Wireless

You can verify the SD-Access wireless configurations using the following commands:

Table 132: Commands for Verifying SD-Access Wireless

Commands	Description
show wireless fabric summary	Displays the fabric status.
show wireless fabric vnid mapping	Displays all the VNID mapping details.
show wireless profile fabric detailed *fabric_profile_name*	Displays the details of a given fabric profile name.
show ap name *AP_name* **config general**	Displays the general details of the Cisco AP.

Commands	Description
show wireless client mac *MAC_addr* **detail**	Displays the detailed information for a client by MAC address.
show wireless tag site detailed *site_tag*	Displays the detailed parameters for a site tag.

CHAPTER 162

Passive Client

- Information About Passive Clients, on page 1789
- Enabling Passive Client on WLAN Policy Profile (GUI), on page 1790
- Enabling Passive Client on WLAN Policy Profile (CLI), on page 1790
- Enabling ARP Broadcast on VLAN (GUI), on page 1791
- Enabling ARP Broadcast on VLAN (CLI), on page 1791
- Configuring Passive Client in Fabric Deployment, on page 1792
- Verifying Passive Client Configuration, on page 1795

Information About Passive Clients

Passive Clients are wireless devices, such as printers and devices configured using a static IP address. Such clients do no transmit any IP information after associating to an AP. That is why, the controller does not learn their IP address unless they perform the DHCP process.

In the controller, the clients just show up in the **Learn IP** state and get timed out because of the DHCP policy-timeout.

The Passive Client feature can be enabled on a per WLAN basis. Enabling this feature will change a few default behaviors in order to better accommodate passive clients. These changes include :

- No client will ever timeout in the IP_LEARN phase. The controller will keep on waiting to learn their IP address. Note that the idle timeout remains active and will delete the client entry after the timeout period expiry, if the client remains silent all along.
- ARP coming from the wired side is broadcasted to all the APs, if the controller does not know the client IP address, to ensure that it reaches the passive client. After this, the controller learns the client IP from the ARP response.

Note In order to save air time, the controller transforms the ARP broadcast coming from the wired side or from other wireless clients and unicasts them to the wireless client it owns . This is only possible after the controller has learned the MAC-IP binding of its wireless client.

When the controller enables ARP broadcast, the controller does not transform the ARP broadcasts into unicasts but only forwards the broadcast, thereby wasting air time for other clients (with a frame that is not acknowledgeable and therefore less reliable). This pushes the passive client to respond to the ARP request and therefore every other client benefits from learning the MAC-IP binding of the wireless client.

Note Passive client feature is not supported on FlexConnect local switching mode.

Enabling Passive Client on WLAN Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy** page, click **Add** to open the **Add Policy Profile** page.

Step 2 In the **General** tab, use the slider to enable **Passive Client**.

Step 3 Click **Save & Apply to Device**.

Enabling Passive Client on WLAN Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**[no] passive-client** **Example:** `Device(config-wireless-policy)# [no] passive-client`	Enables Passive Client.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Enabling ARP Broadcast on VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** page, click **VLAN** tab.
Step 2 Click **Add** to view the **Create VLAN** window.
Step 3 Use the slider to enable **ARP Broadcast**.
Step 4 Click **Save & Apply to Device**.

Enabling ARP Broadcast on VLAN (CLI)

Note ARP Broadcast feature is not supported on VLAN groups.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan configuration** *vlan-id* **Example:** `Device(config)# vlan configuration 1`	Configures a VLAN or a collection of VLANs and enters VLAN configuration mode.
Step 3	**[no] arp broadcast** **Example:** `Device(config-vlan)# [no] arp broadcast`	Enables ARP broadcast on VLAN.
Step 4	**end** **Example:** `Device(config-vlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Passive Client in Fabric Deployment

You need to enable the following for passive client feature to work:

- ARP broadcast on VLANs
- LISP multicast. For information on LISP multicast, see:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-lisp-multicast.html

For information on LISP (Locator ID Separation Protocol), see:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-cfg-lisp.html

Enabling Broadcast Underlay on VLAN

Note You can perform the following configuration tasks from Fabric Edge Node only and not from your controller.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `FabricEdge# configure terminal`	Enters global configuration mode.
Step 2	**router lisp** **Example:** `FabricEdge(config)# router lisp`	Enters LISP configuration mode.
Step 3	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 3`	Creates a LISP EID instance to group multiple services. Configurations under this instance-id are applicable to all services underneath it.
Step 4	**service ipv4** **Example:** `FabricEdge(config-router-lisp-instance)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters the service submode.
Step 5	**database-mapping** *eid* **locator-set** *RLOC name* **Example:**	Configures EID to RLOC mapping relationship.

	Command or Action	Purpose
	`FabricEdge(config-router-lisp-instance-dynamic-eid)# database-mapping 66.66.66.64/32 locator-set rloc1`	
Step 6	**map-cache** *destination-eid* **map-request** **Example:** `FabricEdge(config-router-lisp-instance-service)# map-cache 0.0.0.0/0 map-request`	Generates a static map request for the destination EID.
Step 7	**exit-service-ipv4** **Example:** `FabricEdge(config-router-lisp-instance-service)# exit-service-ipv4`	Exits service submode.
Step 8	**exit-instance-id** **Example:** `FabricEdge(config-router-lisp-instance)# exit-instance-id`	Exits instance submode.
Step 9	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 101`	Creates a LISP EID instance to group multiple services.
Step 10	**service ethernet** **Example:** `FabricEdge(config-router-lisp-instance)# service ethernet`	Enables Layer 2 network services and enters service submode.
Step 11	**eid-table vlan** *vlan-number* **Example:** `FabricEdge(config-router-lisp-instance-service)# eid-table vlan 101`	Associates the LISP instance-id configured earlier with a VLAN through which the endpoint identifier address space is reachable.
Step 12	**broadcast-underlay** *multicast-group* **Example:** `FabricEdge(config-router-lisp-instance-service)# broadcast-underlay 239.0.0.1`	Specifies the multicast group used by the underlay to carry the overlay Layer 2 broadcast traffic.
Step 13	**exit-service-ethernet** **Example:** `FabricEdge(config-router-lisp-instance-service)# exit-service-ethernet`	Exits service sub mode.
Step 14	**exit-instance-id** **Example:** `FabricEdge(config-router-lisp-instance)# exit-instance-id`	Exits instance sub mode.

Enabling ARP Flooding

Note You can perform the following configuration tasks from Fabric Edge Node only and not from your controller.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `FabricEdge# configure terminal`	Enters global configuration mode.
Step 2	**router lisp** **Example:** `FabricEdge(config)# router lisp`	Enters LISP configuration mode.
Step 3	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 3`	Creates a LISP EID instance to group multiple services. Configurations under this instance-id are applicable to all services underneath it.
Step 4	**service ipv4** **Example:** `FabricEdge(config-router-lisp-instance)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters the service submode.
Step 5	**database-mapping** *eid* **locator-set** *RLOC name* **Example:** `FabricEdge(config-router-lisp-instance-dynamic-eid)# database-mapping 66.66.66.64/32 locator-set rloc1`	Configures EID to RLOC mapping relationship.
Step 6	**map-cache** *destination-eid* **map-request** **Example:** `FabricEdge(config-router-lisp-instance-service)# map-cache 0.0.0.0/0 map-request`	Generates a static map request for the destination EID.
Step 7	**exit-service-ipv4** **Example:** `FabricEdge(config-router-lisp-instance-service)# exit-service-ipv4`	Exits service submode.
Step 8	**exit-instance-id** **Example:**	Exits instance submode.

	Command or Action	Purpose
	`FabricEdge(config-router-lisp-instance)# exit-instance-id`	
Step 9	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 101`	Creates a LISP EID instance to group multiple services.
Step 10	**service ethernet** **Example:** `FabricEdge(config-router-lisp-instance)# service ethernet`	Enables Layer 2 network services and enters service submode.
Step 11	**eid-table vlan** *vlan-number* **Example:** `FabricEdge(config-router-lisp-instance-service)# eid-table vlan 101`	Associates the LISP instance-id configured earlier with a VLAN through which the endpoint identifier address space is reachable.
Step 12	**flood arp-nd** **Example:** `FabricEdge(config-router-lisp-instance-service)# flood arp-nd`	Enables ARP flooding.
Step 13	**database-mapping** *mac* **locator-set** *RLOC name* **Example:** `FabricEdge(config-router-lisp-instance-service)# database-mapping mac locator-set rloc1`	Configures EID to RLOC mapping relationship.
Step 14	**exit-service-ethernet** **Example:** `FabricEdge(config-router-lisp-instance-service)# exit-service-ethernet`	Exits service sub mode.
Step 15	**exit-instance-id** **Example:** `FabricEdge(config-router-lisp-instance)# exit-instance-id`	Exits instance sub mode.

Verifying Passive Client Configuration

To verify the status of the Passive Client, use the following command:

```
Device# show wireless profile policy detailed sample-profile-policy

Policy Profile Name           : sample-profile-policy
Description                   : sample-policy
Status                        : ENABLED
```

```
VLAN                          : 20
Client count                  : 0
Passive Client                : ENABLED    <--------------------
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : DISABLED
  Override DNS                : DISABLED
  Override NAT PAT            : DISABLED
  Central Assoc               : DISABLED
.
.
.
```

To verify VLANs that have ARP broadcast enabled, use the following command:

```
Device# show platform software arp broadcast

Arp broadcast is enabled on vlans:
20
```

CHAPTER 163

Fabric in a Box with External Fabric Edge

- Introduction to Fabric in a Box with External Fabric Edge, on page 1797
- Configuring a Fabric Profile (CLI), on page 1797
- Configuring a Policy Profile (CLI) , on page 1798
- Configuring a Site Tag (CLI), on page 1799
- Configuring a WLAN (CLI), on page 1800
- Configuring a Policy Tag (CLI), on page 1800
- Configuring an AP Profile, on page 1801
- Configuring Map Server and AP Subnet (CLI), on page 1801
- Configuring Fabric on FiaB Node, on page 1802
- Configuring a Fabric Edge Node, on page 1808
- Verifying Fabric Configuration, on page 1815

Introduction to Fabric in a Box with External Fabric Edge

From Cisco IOS XE Amsterdam 17.2.1, the Fabric in a Box (FiaB) topology supports external fabric edge nodes. In a fabric-enabled wireless environment using FiaB (border node, control plane, fabric edge, and wireless controller in the same box), you can expand the network by adding external fabric edge nodes. The external fabric edge helps to increase the port density and extend the wireless reach by adding more APs. The APs and clients can exist on both the FiaB and the external fabric edge nodes. Also, the clients can roam between the APs on the FiaB and the external fabric edge nodes.

Configuring a Fabric Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile fabric** *fabric-profile-name* **Example:** `Device(config)# wireless profile fabric test-fabric-profile`	Configures the wireless fabric profile parameters.
Step 3	**client-l2-vnid** *client-l2-vnid* **Example:** `Device(config-wireless-fabric)# client-l2-vnid 8189`	Configures client L2-VNID. Here, *client-l2-vnid* refers to the client L2-VNID value. The valid range is from 0 to 16777215.
Step 4	**description** *description* **Example:** `Device(config-wireless-fabric)# description test-fabric-profile`	Adds a description for the fabric profile.
Step 5	**end** **Example:** `Device(config-wireless-fabric)# end`	Returns to privileged EXEC mode.

Configuring a Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy test-policy-profile`	Configures wireless policy profile and enters wireless policy configuration mode. **Note** In Fabric deployments, local mode, local authentication, and local association are not supported.
Step 3	**no central dhcp** **Example:** `Device(config-wireless-policy)# no central dhcp`	Configures local DHCP mode, where the DHCP is performed in an AP.
Step 4	**no central switching** **Example:**	Configures a WLAN for local switching.

	Command or Action	Purpose
	`Device(config-wireless-policy)# no central switching`	
Step 5	**fabric** *fabric-name* **Example:** `Device(config-wireless-fabric)# fabric test-fabric-profile`	Applies the fabric profile.
Step 6	**no shutdown** **Example:** `Device(config-wireless-fabric)# no shutdown`	Enables the policy profile.
Step 7	**end** **Example:** `Device(config-wireless-fabric)# end`	Returns to privileged EXEC mode.

Configuring a Site Tag (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wireless tag site** *site-tag* **Example:** `Device(config)# wireless tag site default-site-tag-fabric`	Configures site tag and enters site tag configuration mode.
Step 3	**ap-profile** *ap-profile-name* **Example:** `Device(config-site-tag)# ap-profile default-ap-profile-fabric`	Assigns an AP profile to the wireless site.
Step 4	**description** *description* **Example:** `Device(config-site-tag)# description fabric-site`	Adds a description to the AP profile.
Step 5	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode.

Configuring a WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan test-wlan 1 test-wlan`	Configures a WLAN and enters WLAN configuration submode.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring a Policy Tag (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy test-policy-tag`	Configures policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan test-wlan policy test-policy-profile`	Maps a policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-site-tag)# end`	Returns to privileged EXEC mode.

Configuring an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile test-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**ap** *ap-ether-mac* **Example:** `Device(config-ap-profile)# ap 006b.f126.036e`	Enters AP configuration mode.
Step 4	**policy-tag** *policy-tag* **Example:** `Device(config-ap-profile)# policy-tag test-policy-tag`	Specifies the policy tag that is to be attached to the AP.
Step 5	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

Configuring Map Server and AP Subnet (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless fabric** **Example:** `Device(config)# wireless fabric`	Enables SD-Access wireless globally.

	Command or Action	Purpose
Step 3	**wireless fabric name** *name* **l2-vnid** *l2-vnid-value* **l3-vnid** *l3-vnid-value* **ip** *network-ip subnet-mask* **Example:** `Device(config)# wireless fabric name 40_40_0_0-INFRA_VN l2-vnid 8188 l3-vnid 4097 ip 40.40.0.0 255.255.0.0`	Configures AP subnet Layer 2 and Layer 3 VNIDs.
Step 4	**wireless fabric name** *name* **l2-vnid** *l2-vnid-value* **Example:** `Device(config)# wireless fabric name 41_41_0_0-DEFAULT_VN l2-vnid 8189`	Defines client Layer 2 VNID AAA override.
Step 5	**wireless fabric control-plane** *name* **Example:** `Device(config)# wireless fabric control-plane default-control-plane`	Configures the control plane name.
Step 6	**ip address** *ip-address* **key** *shared-key* **Example:** `Device((config-wireless-cp)# ip address 5.5.5.5 key 0 3a18df`	Configures the map server IP address and authentication key shared with the map server.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Fabric on FiaB Node

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `FiaB# configure terminal`	Enters global configuration mode.
Step 2	**router lisp** **Example:** `FiaB(config)# router lisp`	Enters LISP configuration mode.
Step 3	**locator-table default** **Example:**	Associates a default Virtual Routing and Forwarding (VRF) table through which the routing locator address space is reachable to a

	Command or Action	Purpose
	`FiaB(config-router-lisp)# locator-table default`	router Locator ID Separation Protocol (LISP) instantiation.
Step 4	**locator-set** *locator-set-name* **Example:** `FiaB(config-router-lisp)# locator-set WLC`	Specifies a named locator set and enters LISP locator-set configuration mode.
Step 5	*ip-address* **Example:** `FiaB(config-router-lisp-locator-set)# 5.5.5.5`	Specifies an IP address of loopback or other egress tunnel router (ETR) interface.
Step 6	**exit-locator-set** **Example:** `FiaB(config-router-lisp-locator-set)# exit-locator-set`	Exits LISP locator-set configuration mode.
Step 7	**locator-set rloc_loopback** **Example:** `FiaB(config-router-lisp)# locator-set rloc_loopback`	Specifies an existing locator set and enters LISP locator-set configuration mode.
Step 8	**ipv4-interface** *interface* **Example:** `FiaB(config-router-lisp-locator-set)# IPv4-interface Loopback0`	Configures a locator address by creating a locator entry.
Step 9	**auto-discover-rlocs** **Example:** `FiaB(config-router-lisp-locator-set)# auto-discover-rlocs`	Configures the ETR to auto discover the locators registered by other xTRs. (Ingress tunnel router (ITR) and an ETR are known as an xTR.)
Step 10	**exit-locator-set** **Example:** `FiaB(config-router-lisp-locator-set)# exit-locator-set`	Exits LISP locator-set configuration mode.
Step 11	**service ipv4** **Example:** `FiaB(config-router-lisp)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters service submode.
Step 12	**encapsulation vxlan** **Example:** `FiaB(config-lisp-srv-ipv4)# encapsulation vxlan`	Configures VXLAN as encapsulation type for data packets.

	Command or Action	Purpose
Step 13	**itr map-resolver** *map-resolver-address* **Example:** `FiaB(config-lisp-srv-ipv4)# itr map-resolver 5.5.5.5`	Configures map resolver address for sending map requests.
Step 14	**etr map-server** *map-server-address* **key** *key-type authentication-key* **Example:** `FiaB(config-lisp-srv-ipv4)# etr map-server 5.5.5.5 key 7 #########`	Configures the map server for ETR registration.
Step 15	**etr** **Example:** `FiaB(config-lisp-srv-ipv4)# etr`	Configures a LISP ETR.
Step 16	**sgt** **Example:** `FiaB(config-lisp-srv-ipv4)# sgt`	Enables security group tag propagation in LISP-encapsulated traffic.
Step 17	**no map-cache away-eids send-map-request** **Example:** `FiaB(config-lisp-srv-ipv4)# no map-cache away-eids send-map-request`	Removes the address family-specific map cache configuration.
Step 18	**proxy-itr** *ip-address* **Example:** `FiaB(config-lisp-srv-ipv4)# proxy-itr 5.5.5.5`	Enables the Proxy Ingress Tunnel Router (PITR) functionality and specifies the address to use when LISP encapsulating packets to LISP sites.
Step 19	**map-server** **Example:** `FiaB(config-lisp-srv-ipv4)# map-server`	Configures a LISP map server.
Step 20	**map-resolver** **Example:** `FiaB(config-lisp-srv-ipv4)# map-resolver`	Configures a LISP map resolver.
Step 21	**map-cache away-eids send-map-request** **Example:** `FiaB(config-lisp-srv-ipv4)# map-cache 40.40.0.0/16 send-map-request`	Exports table entries into the map cache, with the action set to send-map-request.
Step 22	**route-export site-registrations** **Example:**	Exports LISP site registrations to the routing information base (RIB).

	Command or Action	Purpose
	`FiaB(config-lisp-srv-ipv4)# route-export site-registrations`	
Step 23	**distance site-registrations** *num* **Example:** `FiaB(config-lisp-srv-ipv4)# distance site-registrations 250`	Configures LISP installed routes of type site registrations.
Step 24	**map-cache site-registration** **Example:** `FiaB(config-lisp-srv-ipv4)# map-cache site-registration`	Installs the map cache to a map request for site registrations.
Step 25	**exit-service-ipv4** **Example:** `FiaB(config-lisp-srv-ipv4)# exit-service-ipv4`	Exits LISP service-ipv4 configuration mode.
Step 26	**service ethernet** **Example:** `FiaB(config-router-lisp)# service ethernet`	Selects service type as Ethernet and enters service submode.
Step 27	**database-mapping limit dynamic** *limit* **Example:** `FiaB(config-lisp-srv-eth)# database-mapping limit dynamic 5000`	Configures the maximum number of dynamic local endpoint identifier (EID) prefix database entries.
Step 28	**itr map-resolver** *map-resolver-address* **Example:** `FiaB(config-lisp-srv-eth)# itr map-resolver 5.5.5.5`	Configures the map-resolver address for sending map requests.
Step 29	**itr** **Example:** `FiaB(config-lisp-srv-eth)# itr`	Enables the LISP ITR functionality.
Step 30	**etr map-server** *map-server-address* **key** *key-type authentication-key* **Example:** `FiaB(config-lisp-srv-eth)# etr map-server 5.5.5.5 key 7 1234`	Configures a map server for ETR registration.
Step 31	**etr** **Example:** `FiaB(config-lisp-srv-eth)# etr`	Enables the LISP ETR functionality.

	Command or Action	Purpose
Step 32	**map-server** **Example:** `FiaB(config-lisp-srv-eth)# map-server`	Enables the LISP map server functionality.
Step 33	**map-resolver** **Example:** `FiaB(config-lisp-srv-eth)# map-resolver`	Enables the LISP map resolver functionality.
Step 34	**exit-service-ethernet** **Example:** `FiaB(config-lisp-srv-eth)# exit-service-ethernet`	Exits LISP service-ethernet configuration mode.
Step 35	**instance-id** *instance* **Example:** `FiaB(config-router-lisp)# instance-id 101`	Creates a LISP EID instance to group multiple services.
Step 36	**remote-rloc-probe on-route-change** **Example:** `FiaB(config-lisp-inst)# remote-rloc-probe on-route-change`	Configures the parameters for probing of remote routing locators (RLOCs).
Step 37	**dynamic-eid** *dynamic-eid-name* **Example:** `FiaB(config-lisp-inst)# dynamic-eid 40_40_0_0-INFRA_VN-IPV4`	Configures a dynamic EID and enters dynamic EID configuration mode.
Step 38	**database-mapping** *eid* **locator-set rloc_loopback** **Example:** `FiaB(config-router-lisp-dynamic-eid)# database-mapping 40.40.0.0/16 locator-set rloc_loopback`	Configures EID prefix and locator-set for dynamic EID.
Step 39	**exit-dynamic-id** **Example:** `FiaB(config-router-lisp-dynamic-eid)# exit-dynamic-eid`	Exits LISP dynamic-eid configuration mode.
Step 40	**exit-instance-id** **Example:** `FiaB(config-router-lisp-instance)# exit-instance-id`	Exits LISP instance-id configuration mode.

	Command or Action	Purpose
Step 41	**instance-id** *instance* **Example:** `FiaB(config-router-lisp)# instance-id 101`	Creates a LISP EID instance to group multiple services.
Step 42	**remote-rloc-probe on-route-change** **Example:** `FiaB(config-lisp-inst)# remote-rloc-probe on-route-change`	Configures parameters for probing remote RLOCs.
Step 43	**service ethernet** **Example:** `FiaB(config-lisp-inst)# service ethernet`	Enables Layer 2 network services and enters service submode.
Step 44	**eid-table vlan** *vlan-number* **Example:** `FiaB(config-lisp-inst-srv-eth)# eid-table vlan 101`	Binds an EID table to VLAN.
Step 45	**database-mapping mac locator-set rloc_loopbac** **Example:** `FiaB(config-lisp-inst-srv-eth)# database-mapping mac locator-set rloc_loopbac`	Configures an address family-specific local EID prefixes database.
Step 46	**exit-service-ethernet** **Example:** `FiaB(config-lisp-inst-srv-eth)# exit-service-ethernet`	Exits LISP service-ethernet configuration mode.
Step 47	**exit-instance-id** **Example:** `FiaB(config-lisp-inst)# exit-instance-id`	Exits LISP instance-id configuration mode.
Step 48	**map-server session passive-open** *server* **Example:** `FiaB(config-router-lisp)# map-server session passive-open WLC`	Configures a map server with open passive TCP sockets to listen for incoming connections.
Step 49	**site** *site-name* **Example:** `FiaB(config-router-lisp)# site site_uci`	Configures a LISP site on a map server.
Step 50	**description** *map-server-description* **Example:**	Specifies a description text for the LISP site.

	Command or Action	Purpose
	`FiaB(config-router-lisp-site)# description map-server configured from Cisco DNA-Center`	
Step 51	**authentication-key** *key* **Example:** `FiaB(config-router-lisp-site)# authentication-key 7 ########`	Configures the authentication key used by the LISP site.
Step 52	**eid-record instance-id** *instance-id address* **accept-more-specifics** **Example:** `FiaB(config-router-lisp-site)# eid-record instance-id 4097 0.0.0.0/0 accept-more-specifics`	Specifies that any EID prefix that is more specific than the EID prefix configured is accepted and tracked.
Step 53	**eid-record instance-id** *instance-id* **any-mac** **Example:** `FiaB(config-router-lisp-site)# eid-record instance-id 8188 any-mac`	Accepts registrations, if any, for Layer 2 EID records.
Step 54	**exit-site** **Example:** `FiaB(config-router-lisp-site)# exit-site`	Exits LISP site configuration mode.
Step 55	**ipv4 locator reachability exclude-default** **Example:** `FiaB(config-router-lisp)# ipv4 locator reachability exclude-default`	Configures the IPv4 locator address of the LISP.
Step 56	**ipv4 source-locator** *interface-name* **Example:** `FiaB(config-router-lisp)# ipv4 source-locator Loopback0`	Configures the IPv4 source locator address of the interface.
Step 57	**exit-router-lisp** **Example:** `FiaB(config-router-lisp)# exit-router-lisp`	Exits LISP router-lisp configuration mode.

Configuring a Fabric Edge Node

Note You can perform the following configuration tasks only from Fabric Edge Node, and not from your controller.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `FabricEdge# configure terminal`	Enters global configuration mode.
Step 2	**router lisp** **Example:** `FabricEdge(config)# router lisp`	Enters LISP configuration mode.
Step 3	**locator-table default** **Example:** `FabricEdge(config-router-lisp)# locator-table default`	Associates a default VRF table through which the routing locator address space is reachable to a router LISP instantiation.
Step 4	**locator-set rloc_loopback** **Example:** `FabricEdge(config-router-lisp)# locator-set rloc_loopback`	Specifies a named locator set and enters LISP locator-set configuration mode.
Step 5	**ipv4-interface** *interface-num* **priority** *priority* **weight** *weight* **Example:** `FabricEdge(config-router-lisp-locator-set)# IPv4-interface Loopback 0 priority 10 weight 10`	Configures the IPv4 address of the interface as locator.
Step 6	**exit-locator-set** **Example:** `FabricEdge(config-router-lisp-locator-set)# exit-locator-set`	Exits LISP locator-set configuration mode.
Step 7	**exit-router-lisp** **Example:** `FabricEdge(config-router-lisp-)# exit-router-lisp`	Exits LISP router-lisp configuration mode.
Step 8	**interface vlan** *interface-num* **Example:** `FabricEdge(config)# interface Vlan 2045`	Configures an interface.
Step 9	**description** *description* **Example:** `FabricEdge(config-if)# description Configured from Cisco DNA-Center`	Specifies a description text for the interface.

	Command or Action	Purpose
Step 10	**mac-address** *mac-address* **Example:** `FabricEdge(config-if)# mac-address 0000.0c9f.f85c`	Sets an interface MAC address manually.
Step 11	**ip address** *ip-address mask* **Example:** `FabricEdge(config-if)# ip address 192.168.1.1 255.255.255.252`	Configures an IP address for the interface.
Step 12	**ip helper-address** *ip-address* **Example:** `FabricEdge(config-if)# ip helper-address 9.9.9.9`	Specifies a destination address for UDP broadcasts.
Step 13	**no ip redirects** **Example:** `FabricEdge(config-if)# no ip redirects`	Disables sending of ICMP redirect messages.
Step 14	**ip route-cache same-interface** **Example:** `FabricEdge(config-if)# ip route-cache same-interface`	Enables fast-switching cache for outgoing packets on the same interface.
Step 15	**no lisp mobility liveness test** **Example:** `FabricEdge(config-if)# no lisp mobility liveness test`	Removes liveness test on dynamic EID discovered on this interface.
Step 16	**lisp mobility** *dynamic-eid-name* **Example:** `FabricEdge(config-if)# lisp mobility 40_40_0_0-INFRA_VN-IPV4`	Allows EID mobility on the interface.
Step 17	**exit** **Example:** `FabricEdge(config-if)# exit`	Exits from interface configuration mode.
Step 18	**router lisp** **Example:** `FabricEdge(config)# router lisp`	Enters LISP configuration mode.
Step 19	**locator-set** *locator-set-name* **Example:** `FabricEdge(config-router-lisp)# locator-set rloc_824ecb7`	Specifies a locator set and enters LISP locator-set configuration mode.

	Command or Action	Purpose
Step 20	**exit-locator-set** **Example:** `FabricEdge(config-router-lisp-locator-set)# exit-locator-set`	Exits LISP locator-set configuration mode.
Step 21	**service ipv4** **Example:** `FabricEdge(config-router-lisp)# service ipv4`	Enables Layer 3 network services for the IPv4 address family and enters service submode.
Step 22	**use-petr** *ip-address* **Example:** `FabricEdge(config-lisp-srv-ipv4)# use-petr 5.5.5.5`	Configures the loopback IP address of the Proxy Egress Tunnel Router (PETR).
Step 23	**encapsulation vxlan** **Example:** `FabricEdge(config-lisp-srv-ipv4)# encapsulation vxlan`	Selects the encapsulation type as VXLAN for data packets.
Step 24	**itr map-resolver** *map-resolver-address* **Example:** `FabricEdge(config-lisp-srv-ipv4)# itr map-resolver 5.5.5.5`	Configures the map resolver address for sending map requests.
Step 25	**etr map-server** *map-server-address* **key** *key-type authentication-key* **Example:** `FabricEdge(config-lisp-srv-ipv4)# etr map-server 5.5.5.5 key 7 #########`	Configures the map server for ETR registration.
Step 26	**etr map-server** *map-server-address* **proxy-reply** *authentication-key* **Example:** `FabricEdge(config-lisp-srv-ipv4)# etr map-server 5.5.5.5 proxy-reply`	Configures the locator address of the LISP map server and the authentication key that this router, acting as a LISP ETR, will use to register with the LISP mapping system.
Step 27	**etr** **Example:** `FabricEdge(config-lisp-srv-ipv4)# etr`	Configures a LISP Egress Tunnel Router (ETR).
Step 28	**sgt** **Example:** `FabricEdge(config-lisp-srv-ipv4)# sgt`	Enable security group tag propagation in LISP encapsulated traffic.

	Command or Action	Purpose
Step 29	**no map-cache away-eids send-map-request** **Example:** `FabricEdge(config-lisp-srv-ipv4)# no map-cache away-eids send-map-request`	Removes the address family-specific map cache configuration.
Step 30	**proxy-itr** *ip-address* **Example:** `FabricEdge(config-lisp-srv-ipv4)# proxy-itr 5.5.5.5`	Enables the Proxy Ingress Tunnel Router (PITR) functionality and specifies the address to use when LISP encapsulating packets to LISP sites.
Step 31	**exit-service-ipv4** **Example:** `FabricEdge(config-lisp-srv-ipv4)# exit-service-ipv4`	Exits LISP service-ipv4 configuration mode.
Step 32	**service ethernet** **Example:** `FabricEdge(config-router-lisp)# service ethernet`	Selects the service type as Ethernet.
Step 33	**itr map-resolver** *map-resolver-address* **Example:** `FabricEdge(config-lisp-srv-eth)# itr map-resolver 5.5.5.5`	Configures the map-resolver address for sending map requests.
Step 34	**itr** **Example:** `FabricEdge(config-lisp-srv-eth)# itr`	Enables the LISP ITR functionality.
Step 35	**etr map-server** *map-server-address* **key** *key-type authentication-key* **Example:** `FabricEdge(config-lisp-srv-eth)# etr map-server 5.5.5.5 key 7 1234`	Configures the map server for ETR registration.
Step 36	**etr** **Example:** `FabricEdge(config-lisp-srv-eth)# etr`	Enables the LISP ETR functionality.
Step 37	**exit-service-ethernet** **Example:** `FabricEdge(config-lisp-srv-eth)# exit-service-ethernet`	Exits LISP service-ethernet configuration mode.
Step 38	**instance-id** *instance* **Example:**	Creates a LISP EID instance to group multiple services.

	Command or Action	Purpose
	`FabricEdge(config-router-lisp)# instance-id 101`	
Step 39	**remote-rloc-probe on-route-change** **Example:** `FabricEdge(config-lisp-inst)# remote-rloc-probe on-route-change`	Configures the parameters for probing remote Routing locators (RLOCs).
Step 40	**dynamic-eid** *dynamic-eid-name* **Example:** `FabricEdge(config-lisp-inst)# dynamic-eid 40_40_0_0-INFRA_VN-IPV4`	Configures a dynamic EID and enters dynamic EID configuration mode.
Step 41	**database-mapping** *eid* **locator-set rloc_loopback** **Example:** `FabricEdge(config-router-lisp-dynamic-eid)# database-mapping 40.40.0.0/16 locator-set rloc_loopback`	Configures the EID prefix and locator set for the dynamic EID.
Step 42	**exit-dynamic-id** **Example:** `FabricEdge(config-router-lisp-dynamic-eid)# exit-instance-id`	Exits dynamic instance submode.
Step 43	**service ipv4** **Example:** `FabricEdge(config-lisp-inst)# service ipv4`	Selects service type as IPv4.
Step 44	**eid-table default** **Example:** `FabricEdge(config-lisp-inst-srv-ipv4)# eid-table default`	Binds an EID table.
Step 45	**exit-service-ipv4** **Example:** `FabricEdge(config-lisp-inst-srv-ipv4)# exit-service-ipv4`	Exits LISP service-ipv4 configuration mode.
Step 46	**exit-instance-id** **Example:** `FabricEdge(config-lisp-inst)# exit-instance-id`	Exits LISP instance-id configuration mode.
Step 47	**service ipv4** **Example:**	Selects service type as IPv4.

	Command or Action	Purpose
	`FabricEdge(config-router-lisp)# service ipv4`	
Step 48	**map-cache away-eids map-request** **Example:** `FabricEdge(config-lisp-srv-ipv4)# map-cache 40.40.0.0/16 map-request`	Exports away table entries into the map cache, with the action set to send-map-request.
Step 49	**exit-service-ipv4** **Example:** `FabricEdge(config-lisp-srv-ipv4)# exit-service-ipv4`	Exits LISP service-ipv4 configuration mode.
Step 50	**instance-id** *instance* **Example:** `FabricEdge(config-router-lisp)# instance-id 8188`	Creates a LISP EID instance to group multiple services.
Step 51	**remote-rloc-probe on-route-change** **Example:** `FabricEdge(config-lisp-inst)# remote-rloc-probe on-route-change`	Configures parameters for probing remote RLOCs.
Step 52	**service ethernet** **Example:** `FabricEdge(config-lisp-inst)# service ethernet`	Enables Layer 2 network services and enters service submode.
Step 53	**eid-table vlan** *vlan-number* **Example:** `FabricEdge(config-lisp-inst-srv-eth)# eid-table vlan 101`	Binds an EID table to VLAN.
Step 54	**database-mapping maclocator-set rloc_loopbac** **Example:** `FabricEdge(config-lisp-inst-srv-eth)# database-mapping mac locator-set rloc_loopbac`	Configures address family-specific local EID prefixes database.
Step 55	**exit-service-ethernet** **Example:** `FabricEdge(config-lisp-inst-srv-eth)# exit-service-ethernet`	Exits LISP service-ethernet configuration mode.
Step 56	**exit-instance-id** **Example:**	Exits from LISP instance-id configuration mode.

	Command or Action	Purpose
	`FabricEdge(config-lisp-inst)# exit-instance-id`	
Step 57	**ipv4 locator reachability minimum-mask-length** *length* **Example:** `FabricEdge(config-router-lisp)# ipv4 locator reachability minimum-mask-length 32`	Configures the IPv4 locator address of the LISP.
Step 58	**ipv4 source-locator** *interface-name* **Example:** `FabricEdge(config-router-lisp)# ipv4 source-locator Loopback0`	Configures the IPv4 source locator address of the interface.
Step 59	**exit-router-lisp** **Example:** `FabricEdge(config-router-lisp)# exit-router-lisp`	Exits LISP router-lisp configuration mode.

Verifying Fabric Configuration

Use the following commands to verify the fabric configuration.

To verify the LISP configuration on a device, use the following command:

```
FabricEdge# show running-config | section router lisp

router lisp
 locator-table default
 locator-set default
  exit-locator-set
 !
 locator-set rloc_loopback
  IPv4-interface Loopback0 priority 10 weight 10
  exit-locator-set
 !
 locator default-set rloc_loopback
 service ipv4
  encapsulation vxlan
  itr map-resolver 21.21.21.21
  itr
  etr map-server 21.21.21.21 key tasman
  etr map-server 21.21.21.21 proxy-reply
  etr
  use-petr 21.21.21.21 priority 1 weight 100
  exit-service-ipv4
 !
 service ethernet
  itr map-resolver 5.5.5.5
  itr map-resolver 21.21.21.21
  itr
  etr map-server 21.21.21.21 key tasman
  etr map-server 21.21.21.21 proxy-reply
```

```
 etr
 exit-service-ethernet
!
instance-id 0
 loc-reach-algorithm lsb-reports ignore
 dynamic-eid eid_10_56_25
  database-mapping 10.56.25.0/24 locator-set rloc_loopback
  exit-dynamic-eid
 !
 service ipv4
  eid-table default
  database-mapping 26.26.26.26/32 locator-set rloc_loopback
  exit-service-ipv4
 !
 exit-instance-id
!
instance-id 1
 service ethernet
  eid-table vlan 25
  flood arp-nd
  database-mapping mac locator-set rloc_loopback
  exit-service-ethernet
 !
 exit-instance-id
!
instance-id 101
 service ipv4
  exit-service-ipv4
 !
 exit-instance-id
!
instance-id 8188
 exit-instance-id
!
loc-reach-algorithm lsb-reports ignore
exit-router-lisp
```

To verify the operational status of LISP as configured on a device, use the following command:

```
FabricEdge# show ip lisp

Information applicable to all EID instances:
  Router-lisp ID:                         0
  Locator table:                          default
  Ingress Tunnel Router (ITR):            enabled
  Egress Tunnel Router (ETR):             enabled
  Proxy-ITR Router (PITR):                disabled
  Proxy-ETR Router (PETR):                disabled
  NAT-traversal Router (NAT-RTR):         disabled
  Mobility First-Hop Router:              disabled
  Map Server (MS):                        disabled
  Map Resolver (MR):                      disabled
  Mr-use-petr:                            disabled
  Delegated Database Tree (DDT):          disabled
  Publication-Subscription:               enabled
    Publisher(s):                         *** NOT FOUND ***
  ITR Map-Resolver(s):                    21.21.21.21
  ETR Map-Server(s):                      21.21.21.21
  xTR-ID:                                 0xD89893A6-0x98749B2C-0x89810431-0x92F33C9C
  site-ID:                                unspecified
  ITR local RLOC (last resort):           *** NOT FOUND ***
  ITR use proxy ETR RLOC(Encap IID):      21.21.21.21
  ITR Solicit Map Request (SMR):          accept and process
    Max SMRs per map-cache entry:         8 more specifics
```

```
    Multiple SMR suppression time:          20 secs
  ETR accept mapping data:                  disabled, verify disabled
  ETR map-cache TTL:                        1d00h
  Locator Status Algorithms:
    RLOC-probe algorithm:                   disabled
    RLOC-probe on route change:             N/A (periodic probing disabled)
    RLOC-probe on member change:            disabled
    LSB reports:                            ignore
    IPv4 RLOC minimum mask length:          /0
    IPv6 RLOC minimum mask length:          /0
  Map-cache:
    Map-cache limit:                        32768
    Map-cache activity check period:        60 secs
    Persistent map-cache:                   disabled
  Source locator configuration:
    GigabitEthernet1/0/1: 24.24.24.24 (Loopback0)
    Vlan25: 24.24.24.24 (Loopback0)
  Database:
    Dynamic database mapping limit:         25000
```

To verify the operational status of the map cache on a device configured as an ITR or PITR, use the following command:

```
FabricEdge# show lisp instance-id iid ipv4 map-cache

LISP IPv4 Mapping Cache for EID-table default (IID 0), 5 entries

0.0.0.0/0, uptime: 2w5d, expires: never, via static-send-map-request
  Encapsulating to proxy ETR

10.56.25.0/24, uptime: 2w0d, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR

10.56.25.25/32, uptime: 2w5d, expires: 23:10:06, via map-reply, complete
  Locator      Uptime    State  Pri/Wgt     Encap-IID
  21.21.21.21  2w5d      up       0/0         -

22.0.0.0/8, uptime: 2w5d, expires: 00:04:54, via map-reply, forward-native
  Encapsulating to proxy ETR

26.26.26.26/32, uptime: 09:48:33, expires: 14:11:26, via map-reply, self, complete
  Locator      Uptime    State     Pri/Wgt     Encap-IID
  24.24.24.24  09:48:33  up, self   50/50        -
```

To verify the operational status of the database mapping on a device configured as an ETR, use the following command:

```
FabricEdge# show lisp instance-id iid ipv4 database

LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 3, no-route 0, inactive 0

10.56.25.27/32, dynamic-eid eid_10_56_25, skip reg, inherited from default locator-set
rloc_loopback
  Uptime: 00:25:11, Last-change: 00:25:11
  Domain-ID: unset
  Locator      Pri/Wgt  Source     State
  24.24.24.24   10/10   cfg-intf   site-self, reachable

10.56.25.67/32, dynamic-eid eid_10_56_25, inherited from default locator-set rloc_loopback
  Uptime: 00:24:47, Last-change: 00:24:47
  Domain-ID: unset
  Locator      Pri/Wgt  Source     State
```

```
  24.24.24.24   10/10   cfg-intf   site-self, reachable

26.26.26.26/32, locator-set rloc_loopback
  Uptime: 2w5d, Last-change: 00:50:36
  Domain-ID: unset
  Locator      Pri/Wgt  Source     State
  24.24.24.24   10/10   cfg-intf   site-self, reachable
```

To verify the configured LISP sites on a LISP map server, use the following command:

```
FabricEdge# show lisp instance-id iid ipv4 server

LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
eca            never     no     --                   0        10.56.25.0/24
               04:52:53  yes#   21.21.21.21:40875    0        10.56.25.25/32
               04:07:09  yes#   27.27.27.27:24949    0        10.56.25.64/32
               03:21:16  yes#   24.24.24.24:23672    0        10.56.25.67/32
               04:52:53  yes#   21.21.21.21:40875    0        23.23.23.23/32
               03:47:04  yes#   24.24.24.24:23672    0        26.26.26.26/32
               2w0d      yes#   27.27.27.27:24949    0        29.29.29.29/32
site_uci       never     no     --                   4097     0.0.0.0/0
```

To verify the operational status of LISP sites, use the following command in FiaB node:

```
FabricEdge# show lisp instance-id 1 ethernet server

================================================
Output for router lisp 0 instance-id 1
================================================
LISP Site Registration Information


================================================
Output for router lisp 0 instance-id 1
================================================
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
eca            never     no     --                   1        any-mac
               04:10:37  yes#   27.27.27.27:24949    1        00b0.e19c.2578/48
               04:09:20  yes#   22.22.22.22:64083    1        00b0.e19c.fc40/48
               03:24:52  yes#   24.24.24.24:23672    1        dcce.c130.0b70/48
               03:23:39  yes#   22.22.22.22:64083    1        dcce.c130.9820/48
```

To verify the operational status of LISP sites, use the following command in FiaB node:

```
FabricEdge# show lisp instance-id 0 ipv4 server

LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
```

```
eca             never     no     --                   0        10.56.25.0/24
                6d18h     yes#   21.21.21.21:40875    0        10.56.25.25/32
                01:23:56  yes#   27.27.27.27:24949    0        10.56.25.64/32
                00:24:40  yes#   24.24.24.24:23672    0        10.56.25.72/32
                6d18h     yes#   21.21.21.21:40875    0        23.23.23.23/32
                6d17h     yes#   24.24.24.24:23672    0        26.26.26.26/32
                3w0d      yes#   27.27.27.27:24949    0        29.29.29.29/32
```

To verify the operational status of LISP sites on IPv4 database, use the following command in fabric edge node:

```
FabricEdge# show lisp instance-id 0 ipv4 database

LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 3, no-route 0, inactive 0

10.56.25.27/32, dynamic-eid eid_10_56_25, skip reg, inherited from default locator-set
rloc_loopback
  Uptime: 00:25:54, Last-change: 00:25:54
  Domain-ID: unset
  Locator      Pri/Wgt  Source     State
  24.24.24.24   10/10   cfg-intf   site-self, reachable
10.56.25.72/32, dynamic-eid eid_10_56_25, inherited from default locator-set rloc_loopback
 Uptime: 00:25:25, Last-change: 00:25:25
  Domain-ID: unset
  Locator      Pri/Wgt  Source     State
  24.24.24.24   10/10   cfg-intf   site-self, reachable
26.26.26.26/32, locator-set rloc_loopback
  Uptime: 3w5d, Last-change: 6d17h
  Domain-ID: unset
  Locator      Pri/Wgt  Source     State
  24.24.24.24   10/10   cfg-intf   site-self, reachable
```

To verify the operational status of LISP sites on mac mapping database, use the following command on the FE node:

```
FabricEdge# show lisp instance-id 1 ethernet database

LISP ETR MAC Mapping Database for EID-table Vlan 25 (IID 1), LSBs: 0x1
Entries total 2, no-route 0, inactive 0

cc98.911b.73f1/48, dynamic-eid Auto-L2-group-1, skip reg, inherited from default locator-set
 rloc_loopback
  Uptime: 00:00:49, Last-change: 00:00:49
  Domain-ID: unset
  Locator      Pri/Wgt  Source     State
  24.24.24.24   10/10   cfg-intf   site-self, reachable
dcce.c130.0b70/48, dynamic-eid Auto-L2-group-1, inherited from default locator-set
rloc_loopback
  Uptime: 00:00:50, Last-change: 00:00:50
  Domain-ID: unset
  Locator      Pri/Wgt  Source     State
  24.24.24.24   10/10   cfg-intf   site-self, reachable
```

PART XVI

VLAN

- VLANs, on page 1823
- VLAN Groups, on page 1833

CHAPTER 164

VLANs

- Information About VLANs, on page 1823
- How to Configure VLANs, on page 1827
- Monitoring VLANs, on page 1831

Information About VLANs

Logical Networks

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any controller port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a controller supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information.

VLANs are often associated with IP subnet. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the controller is assigned manually on an interface-by-interface basis. When you assign controller interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Supported VLANs

The controller supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1 to 4094. VLAN 1 is the default VLAN and is created during system initialization. All of the VLANs except 1002 to 1005 are available for user configuration.

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong.

When a port belongs to a VLAN, the controller learns and manages the addresses associated with the port on a per-VLAN basis.

Table 133: Port Membership Modes and Characteristics

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the controller connected to a trunk port of a second controller.
Trunk IEEE 802.1Q) : • IEEE 802.1Q—Industry-standard trunking encapsulation.	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other controller over trunk links.

Note If a client VLAN has two subnets, a primary subnet and a secondary subnet, the static IP address is not supported on the secondary subnet.

Consider the following SVI configuration example:

interface VlanX

ip address a.b.c.254 255.255.255.0 secondary

ip address a.d.e.254 255.255.255.0

In this scenario, you can't allocate the secondary subnet for clients with static IP addresses.

VLAN Configuration Files

Configurations for VLAN IDs 1 to 1005 are written to the vlan.dat file (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in flash memory. If the VTP mode is transparent, they are also saved in the controller running configuration file.

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the controller, the controller configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the VLAN IDs 1 to 1005 use the VLAN database information.
- In VTP versions 1 and 2, if VTP mode is server, the domain name and VLAN configuration for VLAN IDs 1 to 1005 use the VLAN database information. VTP version 3 also supports VLANs 1006 to 4094.

Note Ensure that you delete the vlan.dat file along with the configuration files before you reset the switch configuration using **write erase** command. This ensures that the switch reboots correctly on a reset.

Normal-Range VLAN Configuration Guidelines

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- Normal-range VLANs are identified with a number between 1 and 1001.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configurations are also saved in the running configuration file.
- If the controller is in VTP server or VTP transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)
- Extended-range VLANs created in VTP transparent mode are not saved in the VLAN database and are not propagated. VTP version 3 supports extended range VLAN (VLANs 1006 to 4094) database propagation in VTP server mode.

If clients are unable to connect to the controller due to a VLAN failure, try one of the following options:

- Configure *ip4 dhcp required* in the policy profile forcing the client to initiate a DHCP request.
- Configure the RADIUS server to send VLAN group (having the client's static IP VLAN) information allowing the client to use static IP.
- Configure *aaa-override vlan fallback* under the policy profile forcing the controller to check for the client's static IP VLAN in other VLAN groups as well. The client can join the network if the client's static IP VLAN is part of the configured VLAN group under the policy profile.

Extended-Range VLAN Configuration Guidelines

Extended-range VLANs are VLANs with IDs from 1006 to 4094.

Follow these guidelines when creating extended-range VLANs:

- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP unless the device is running VTP version 3.
- You cannot include extended-range VLANs in the pruning eligible range.
- For VTP version 1 or 2, you can set the VTP mode to transparent in global configuration mode. You should save this configuration to the startup configuration so that the device boots up in VTP transparent

mode. Otherwise, you lose the extended-range VLAN configuration if the device resets. If you create extended-range VLANs in VTP version 3, you cannot convert to VTP version 1 or 2.

Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

- To configure VLAN through the Web UI, you must change the number of available Virtual Terminal (VTY) sessions to 50. Web UI uses VTY lines for processing HTTP requests. At times, when multiple connections are open, the default VTY lines of 15 set by the device gets exhausted. Therefore, you must change the VTY lines to 50 before using the Web UI.

Note To increase the VTY lines in a device, run the following command in the configuration mode:

```
Device# configure terminal
Device(config)# service tcp-keepalives in
Device(config)# service tcp-keepalives out

Device# configure terminal
Device(config)# line vty 16-50
```

Note The maximum number of SSH VTY sessions supported on the standby controller is eight.

- Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.
- Before adding a VLAN to a VLAN group, you should first create it on the device.

Restrictions for VLANs

The following are restrictions for VLANs:

- You cannot delete a wireless management interface, if the associated VLAN interface is already deleted. To avoid this scenario, you should delete the wireless management interface before deleting the VLAN interface.
- The device supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.
- When client VLAN is not configured for a policy profile, AP native VLAN is used.
- The behavior of VLAN 1 changes depending on the AP mode. These scenarios are described below:
  - **Local mode AP**: If you use *vlan-name*, clients are assigned to VLAN 1. However, if you use *vlan-id* 1, clients are assigned to the wireless management interface.
  - **FlexConnect mode AP**: If you use *vlan-name*, clients are assigned to VLAN 1. However, if you use *vlan-id* 1, clients are assigned to the native VLAN defined in the flex profile.

By default, the policy profile assigns vlan-id 1 so that clients can use the wireless management VLAN.

- You cannot use the same VLAN on the same SSID for local switching and central switching.

How to Configure VLANs

How to Configure Normal-Range VLANs

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type
  - Ethernet
  - TrBRF or TrCRF
- VLAN state (active or suspended)
- Parent VLAN number for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

You can cause inconsistency in the VLAN database if you attempt to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, follow the procedures in this section.

Creating or Modifying an Ethernet VLAN

Before you begin

With VTP version 1 and 2, if the controller is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

The controller supports only Ethernet interfaces.

Procedure

	Command or Action	Purpose
Step 1	**vlan** *vlan-id* **Example:** `Device(config)# vlan 20`	Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. **Note** The available VLAN ID range for this command is 1 to 4094.

	Command or Action	Purpose
Step 2	**name** *vlan-name* **Example:** `Device(config-vlan)# name test20`	(Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 3	**media** { **ethernet** | **fd-net** | **trn-net** } **Example:** `Device(config-vlan)# media ethernet`	Configures the VLAN media type.
Step 4	**show vlan** {**name** *vlan-name* | **id** *vlan-id*} **Example:** `Device# show vlan name test20 id 20`	Verifies your entries.

Assigning Static-Access Ports to a VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** > **VLAN**

Step 2 Click the **VLAN** tab.

Step 3 To assign **Port Members**, click the interfaces that are to be included as port members from the **Available** list and click on the arrow to move it to the **Associated** list.

Step 4 Click **Update & Apply to Device**.

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode). For more information on static-access ports, see *VLAN Port Membership Modes*.

If you assign an interface to a VLAN that does not exist, the new VLAN is created.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode

	Command or Action	Purpose
Step 2	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet2/0/1`	Enters the interface to be added to the VLAN.
Step 3	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Defines the VLAN membership mode for the port (Layer 2 access port).
Step 4	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 2`	Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id* **Example:** `Device# copy running-config startup-config`	Verifies the VLAN membership mode of the interface.
Step 7	**show interfaces** *interface-id* **switchport** **Example:** `Device# show interfaces gigabitethernet2/0/1`	Verifies your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.

How to Configure Extended-Range VLANs

Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any **switchport** commands that allow VLAN IDs.

With VTP version 1 or 2, extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the controller running configuration file, and you can

save the configuration in the startup configuration file. Extended-range VLANs created in VTP version 3 are stored in the VLAN database.

Creating an Extended-Range VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN**.

Step 2 In the VLAN page, click **ADD**.

Step 3 Enter the extended range VLAN ID in the **VLAN ID** field.

The extended range is between range is 1006 and 4094.

Step 4 Enter a VLAN name in the **Name** field.

Step 5 Save the configuration.

Creating an Extended-Range VLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan** *vlan-id* **Example:** `Device(config)# vlan 2000`	Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.
Step 3	**show vlan id** *vlan-id* **Example:** `Device# show vlan id 2000`	Verifies that the VLAN has been created.

Monitoring VLANs

Table 134: Privileged EXEC show Commands

Command	Purpose
show interfaces [**vlan** *vlan-id*]	Displays characteristics for all interfaces or for the specified VLAN configured on the controller.
show vlan [**access-map** *name* | **brief** | **group** |**id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **summary**]	Displays parameters for all VLANs or the specified VLAN on the controller. The following command options are available: • **brief**—Displays VTP VLAN status in brief. • **group**—Displays the VLAN group with its name and the connected VLANs that are available. • **id**—Displays VTP VLAN status by identification number. • **ifindex**—Displays SNMP ifIndex. • **mtu**—Displays VLAN MTU information. • **name**—Displays the VTP VLAN information by specified name. • **summary**—Displays a summary of VLAN information.

CHAPTER 165

VLAN Groups

- Information About VLAN Groups, on page 1833
- Prerequisites for VLAN Groups, on page 1834
- Restrictions for VLAN Groups, on page 1834
- Creating a VLAN Group (GUI), on page 1834
- Creating a VLAN Group (CLI), on page 1835
- Adding a VLAN Group to Policy Profile (GUI), on page 1835
- Adding a VLAN Group to a Policy Profile, on page 1836
- Viewing the VLANs in a VLAN Group, on page 1836
- VLAN Group Support for DHCP and Static IP Clients, on page 1837

Information About VLAN Groups

Whenever a client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the policy profile mapped to the WLAN. In a large venue, such as an auditorium, a stadium, or a conference room where there are numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN group feature uses a single policy profile that can support multiple VLANs. The clients can get assigned to one of the configured VLANs. This feature maps a policy profile to a single VLAN or multiple VLANs using the VLAN groups. When a wireless client associates to the WLAN, the VLAN is derived by an algorithm based on the MAC address of the wireless client. A VLAN is assigned to the client and the client gets the IP address from the assigned VLAN.

The system marks VLAN as *Dirty* for 30 minutes when the clients are unable to receive IP addresses using DHCP. The system might not clear the *Dirty* flag from the VLAN even after 30 minutes for a VLAN group. After 30 minutes, when the VLAN is marked non-dirty, new clients in the IP Learn state can get assigned with IP addresses from the VLAN if free IPs are available in the pool and DHCP scope is defined correctly. This is the expected behavior because the timestamp of each interface has to be checked to see if it is greater than 30 minutes, due to which there is a lag of 5 minutes for the global timer to expire.

Note The Controller marks the VLAN interface as *Dirty* when three or more clients fail to receive IP addresses through DHCP. The VLAN interface is deemed *Dirty* using the Non-Aggressive method, which involves counting one failure per association per client that surpasses the predefined **IP_LEARN_TIMEOUT** duration of 120 seconds. If a client sends a new association request before the **IP_LEARN_TIMEOUT** elapses, it will not be considered a failed client.

In Non-Aggressive method, each client gets a unique hash value derived from its MAC address. This approach ensures that clients belonging to the same vendor, which may differ only by a few bits, do not mistakenly trigger the *Dirty* marking of a VLAN.

Prerequisites for VLAN Groups

- A VLAN should be present in the device for it to be added to the VLAN group.

Restrictions for VLAN Groups

- If the number of VLANs in a VLAN group exceeds 32, the mobility functionality might not work as expected and Layer 2 multicast might break for some VLANs. Therefore, it is the responsibility of network administrators to configure a feasible number of VLANs in a VLAN group.

  For the VLAN Groups feature to work as expected, the VLANs mapped in a group must be present in the controller.

- The VLAN Groups feature works for access points in local mode.
- The VLAN Groups feature works only in central switching mode and it cannot be used in FlexConnect local switching mode.
- ARP Broadcast feature is not supported on VLAN groups.
- VLAN group Multicast with VLAN group is only supported in local mode AP. Multicast VLAN is required when VLAN group is configured and uses multicast traffic.
- While you configure VLAN groups with multiple VLANs and each VLAN is used by a different subnet, clients having static IP addresses might be assigned to a wrong VLAN if SVIs are not present on the controller. Hence, for every VLAN that belongs to the VLAN group, ensure that you configure an SVI interface with a valid IP address.

Creating a VLAN Group (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN**

Step 2 On the **VLAN** > **VLAN** page, click **Add**.

Step 3 Enter the VLAN ID in the **VLAN ID** field.

The valid range is between 2 and 4094.

Step 4 Enter the VLAN name in the **Name** field.

Configure the other parameters if required.

Step 5 Click **Update & Apply to Device**.

Creating a VLAN Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan group** *WORD* **vlan-list** *vlan-ID* **Example:** `Device(config)#vlan group vlangrp1 vlan-list 91-95`	Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the maximum number of VLANs supported in a group is 64.
Step 3	**end** **Example:** `Device(config)#end`	Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Adding a VLAN Group to Policy Profile (GUI)

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for the client that is applied on the AP or controller is moved to the policy profile. For example, VLAN, ACL, QOS, Session timeout, Idle timeout, AVC profile, Bonjour profile, Local profiling, Device classification, BSSID QoS, etc. However, all wireless related security attributes and features on the WLAN are grouped under the WLAN profile.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the**Policy Profile** page, click on a policy profile name.

Step 3 Click **Access Policies** tab.

Step 4 Under **VLAN** section, use the **VLAN/VLAN Group** drop-down list to select a VLAN or VLAN Group.

Step 5 Click **Update & Apply to Device**.

Adding a VLAN Group to a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)# wireless profile policy my-wlan-policy`	Configures the WLAN policy profile.
Step 3	**vlan** *vlan-group1* **Example:** `Device(config-wireless-policy)# vlan myvlan-group`	Maps the VLAN group to the WLAN by entering the group name.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Viewing the VLANs in a VLAN Group

Command	Description
show vlan group	Displays the list of VLAN groups with name and the VLANs that are configured.
show vlan group group-name *group_name*	Displays the specified VLAN group details.
show wireless client mac-address *client-mac-addr* **detail**	Displays the VLAN group assigned to the client.
show wireless vlan details	Displays VLAN details.

VLAN Group Support for DHCP and Static IP Clients

When a static IP client joins a VLAN group, the controller adds it to a VLAN based on VLAN computation logic. If the client's static IP address isn't part of the VLAN's IP list, the client fails to get internet access, even if the client is authenticated and authorized. The VLAN Group to Support DHCP and Static IP Clients feature aims to handle the network access of such clients. This feature only supports IPv4 clients and is enabled by default. However, ensure that the **ipv4 dhcp required** command is not configured on the wireless policy profile, because this disables the feature, causing the client to be stuck in the IP learn state.

Prerequisites

- Ensure that a switch VLAN interface (SVI) is configured with the IP address.

Restrictions

- FlexConnect local switching and FlexConnect local authentication are not supported. Only Local mode, FlexConnect central switching, and FlexConnect central authentication are supported.
- IPv6 is not supported.
- The peer controller cannot have a VLAN group in the policy profile, because a VLAN group with static IP mobility is not supported.

Supported Features

Table 135: Supported Features

Feature	Support
Guest Anchor	Yes
Mobility	Yes
RLAN	Yes
SVI	Yes Ensure that you configure SVI with an IP address in the same subnet as that of the client's IP address.
IRCM support: Guest AireOS as anchor and Cisco Catalyst 9800 controller as foreign	Yes
IRCM support : Guest AireOS as foreign and Cisco Catalyst 9800 controller as anchor	Yes The client is excluded if there is no match for the SVI.

PART XVII

WLAN

- WLANs, on page 1841
- WLAN Security, on page 1871
- Remote LANs, on page 1885
- RLAN External Module, on page 1903
- 802.11ax Per WLAN, on page 1905
- BSS Coloring, on page 1909
- DHCP for WLANs, on page 1917
- Aironet Extensions IE (CCX IE) , on page 1937
- Device Analytics, on page 1941
- Device Classifier Dynamic XML Support, on page 1947
- BSSID Counters, on page 1955
- Fastlane+, on page 1959
- Workgroup Bridges, on page 1963
- Peer-to-Peer Client Support, on page 1987
- Deny Wireless Client Session Establishment Using Calendar Profiles, on page 1989
- Ethernet over GRE , on page 1999
- Wireless Guest Access, on page 2017
- Wired Guest Access, on page 2047
- Express Wi-Fi by Facebook, on page 2067
- User Defined Network, on page 2077
- Hotspot 2.0, on page 2085
- Client Roaming Across Policy Profile, on page 2111
- Assisted Roaming, on page 2119
- 802.11r BSS Fast Transition, on page 2125

• 802.11v, on page 2141

CHAPTER 166

WLANs

- Information About WLANs, on page 1841
- Prerequisites for WLANs, on page 1844
- Restrictions for WLANs, on page 1844
- How to Configure WLANs, on page 1846
- Verifying WLAN Properties (CLI), on page 1868
- Verifying WLAN-VLAN Information for an AP, on page 1868
- Verifying a WLAN Radio Policy, on page 1869

Information About WLANs

This feature enables you to control WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different access points for better manageability.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the device to access.

Note The **wireless client max-user-login concurrent** command will work as intended even if the **no configure max-user-identity response** command is configured.

Note We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.

Note From Cisco IOS XE Cupertino 17.7.1 release onwards, only 8 WLANs are broadcasted on 6-GHz band.

Note For C9105, C9115, and C9120 APs, when a new WLAN is pushed from the controller and if the existing WLAN functional parameters are changed, the other WLAN clients will disconnect and reconnect.

Band Selection

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the device.

Off-Channel Scanning Deferral

A lightweight access point, in normal operational conditions, periodically goes off-channel and scans another channel. This is in order to perform RRM operations such as the following:

- Transmitting and receiving Neighbor Discovery Protocol (NDP) packets with other APs.
- Detecting rogue APs and clients.
- Measuring noise and interference.

During the off-channel period, which normally is about 70 milliseconds, the AP is unable to transmit or receive data on its serving channel. Therefore, there is a slight impact on its performance and some client transmissions might be dropped.

While the AP is sending and receiving important data, it is possible to configure off-channel scanning deferral so that the AP does not go off-channel and its normal operation is not impacted. You can configure off-channel scanning deferral on a per-WLAN basis, per WMM UP class basis, with a specified time threshold in milliseconds. If the AP sends or receives, on a particular WLAN, a data frame marked with the given UP class within the specified threshold, the AP defers its next RRM off-channel scan. For example, by default, off-channel scanning deferral is enabled for UP classes 4, 5, and 6, with a time threshold of 100 millseconds. Therefore, when RRM is about to perform an off-channel scan, a data frame marked with UP 4, 5, or 6 is received within the last 100 milliseconds, RRM defers going off-channel. The AP radio does not go off-channel when a voice call sending and receiving audio samples is marked as UP class 6 for every active 20 milliseconds.

Off-channel scanning deferral does come with a tradeoff. Off-channel scanning can impact throughput by 2 percent or more, depending on the configuration, traffic patterns, and so on. Throughput can be slightly improved if you enable off-channel scanning deferral for all traffic classes and increase the time threshold. However, by not going off-channel, RRM can fail to identify AP neighbors and rogues, resulting in negative impact to security, DCA, TPC, and 802.11k messages.

DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit broadcast and multicast frames after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames for 10 times every second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames for 5 times every second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon). The only recommended DTIM values are 1 and 2; higher DTIM values will likely cause communications problems.

Note A beacon period, which is specified in milliseconds on the device, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. Depending on the AP model, the actual beacon period may vary slightly; for example, a beacon period of 100 ms may in practice equate to 104.448 ms.

WLAN Radio Policy

The existing WLAN feature allows you to broadcast WLAN on a specified radio on all the applicable slots. With the WLAN Radio Policy feature, you can broadcast the WLAN on the corresponding slot. Note that this option is supported only on 5-GHz band.

Restrictions for WLAN Radio Policy

- WLAN is pushed to all the radios only if the following configuration is used:
  - WPA3 + AES cipher + 802.1x-SHA256 AKM
  - WPA3 + AES cipher + OWE AKM
  - WPA3 + AES cipher + SAE AKM
  - WPA3 + CCMP256 cipher + SUITEB192-1X AKM
  - WPA3 + GCMP256 cipher + SUITEB-1X AKM
  - WPA3 + GCMP128 cipher + SUITEB192-1X AKM

Prerequisites for Configuring Cisco Client Extensions

- The software supports CCX versions 1 through 5, which enables devices and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the device and cannot be disabled. However, you can configure Aironet information elements (IEs).
- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the device sends Aironet IEs 0x85 and 0x95 (which contains the management IP address

of the device and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the device, dropped by the device, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.

Note Peer-to-peer blocking feature is VLAN-based. WLANs using the same VLAN has an impact, if Peer-to-peer blocking feature is enabled.

Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the device GUI or CLI to enable the diagnostic channel, and you can use the device **diag-channel** CLI to run the diagnostic tests.

Note We recommend that you enable the diagnostic channel feature only for non-anchored SSIDs that use the management interface. CCX Diagnostic feature has been tested only with clients having Cisco ADU card

Prerequisites for WLANs

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point (AP) does not advertise disabled WLANs in its access point group or WLANs that belong to another group.
- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that devices properly route VLAN traffic.

Restrictions for WLANs

- Do not configure PSK and CCKM in a WLAN, as this configuration is not supported and impacts client join flow.
- Ensure that TKIP or AES ciphers are enabled with WPA1 configuration, else ISSU may break during upgrade process.

- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- The WLAN name and SSID can have up to 32 characters.
- WLAN and SSID names support only the following ASCII characters:
  - Numerals: 48 through 57 hex (0 to 9)
  - Alphabets (uppercase): 65 through 90 hex (A to Z)
  - Alphabets (lowercase): 97 through 122 hex (a to z)
  - ASCII space: 20 hex
  - Printable special characters: 21 through 2F, 3A through 40, and 5B through 60 hex, that is: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.
- In a dual-stack with IPv4 and IPv6 configured in the Cisco 9800 controller, if an AP tries to join controller with IPv6 tunnel before its IPv4 tunnel gets cleaned, you would see a traceback and AP join will fail.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.
- The SSID that is sent as part of the user profile will work only if **aaa override** command is configured.
- RADIUS server overwrite is not configured on a per WLAN basis, but rather on a per AAA server group basis.
- Downloadable ACL (DACL) is supported only on the central switching mode. It is not supported for Flex Local switching or on the Cisco Embedded Wireless Controller.
- You cannot mix open configuration models with CLI-based, GUI-based, or Catalyst Center-based configurations. However, if you decide to use multiple model types, they must remain independent of each other. For example, in open configuration models, you can only manage configurations that have been created using an open configuration model, not a CLI-based or GUI-based model. Configurations that are created using open configuration models cannot be modified using a GUI-based model, or CLI-based model, or any other model.

- When you are configuring **dot11bg 11g** command and **radio dot11bg** or **radio dot11g** command, the clients can still connect in 5GHz radio. In this scenario, the client association needs to be blocked. This option is only available on a 2.4-GHz radio.

Caution Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this WLAN feature with care.

How to Configure WLANs

WLAN Wizard

A wireless local-area network (WLAN) is a group of devices that form a network based on radio transmissions rather than wired connections. The WLAN Wizard on the WebUI is a simplified workflow designed to help you quickly create a WLAN and setup some primary configurations for your specific deployment.

The Wizard supports the following wireless deployment modes:

- Local mode: In Local mode, the WLAN is broadcast in the campus locally.
- Flex Connect mode: In FlexConnect mode, the WLAN is broadcast remotely across the WAN in a branch.
- Guest CWA mode: In Guest CWA mode, the WLAN is created for guest access with Central Web Authentication (CWA).

There are different authentication methods supported for each deployment mode.

To configure a WLAN for your preferred wireless deployment mode using the WLAN wizard on the WebUI, go to **Configuration > Wireless Setup > WLAN Wizard**.

You can also navigate to the WLAN Wizard by the following paths:

- On the Toolbar, click on the **Wireless Setup** icon and select **WLAN Wizard** from the drop-down list.
- On the left navigation pane, go to **Configuration > Tags & Profiles > WLANs** and click on **WLAN Wizard** on the top-right corner.

On the **WLAN Wizard** page, select a wireless deployment mode for the WLAN to initiate steps for setting up the WLAN with profiles, authentication methods, tags, and APs and other configurations.

Local Mode

The WLAN is deployed in Local mode when the WLAN is present in an office setup with no branch offices. In local mode, an AP creates two CAPWAP tunnels to the controller. One is for management, the other is data traffic. This behavior is known as "centrally switched" because the data traffic is tunneled (bridged) from the AP to the controller where it is then routed by some routing device. Locally switched means the traffic is terminated at the local switch adjacent to the access point.

Authentication Method

To configure a WLAN for local mode, select the preferred authentication method from the left panel. The authentication method sets the method by which a client can access the WLAN and decides the level of security on the WLAN. The options are:

- PSK: A Pre-Shared Key (PSK) is a unique key created for individuals or groups of users on the same SSID. A client will have to enter the PSK to be authenticated and allowed to access the WLAN.
- Dot1x: The client must go through relevant EAP authentication model to start exchanging traffic in the WLAN.
- Local Web Authentication: The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication.
- External Web Authentication: The controller intercepts htttp(s) traffic and redirects the client to the login page hosted on the external web server for authentication.
- Central Web Authentication: The controller redirects all web traffic from the client to the ISE login page for authentication.

WLAN Profile and Policy

After selecting the Authentication method, click on **WLAN** on the left panel to enter the WLAN profile and policy details.

The WLAN profile defines the properties of a WLAN such as Profile Name, Status, WLAN ID, L2 and L3 Security parameters, AAA Server associated with this SSID and other parameters that are specific to a particular WLAN. The policy profile defines the network policies and the switching policies for a client (with the exception of QoS), which constitute the AP policies as well.

Procedure

Step 1 In the **Network Name** section, enter a **WLAN profile name**, which is a unique name for your wireless network. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 2 Enter a valid **SSID** for the WLAN. A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.

Step 3 Enter the **WLAN ID**.

Step 4 In the **WLAN Policy** section, enter the **Policy Profile name**. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 5 Select the **VLAN** to be associated with the Policy Profile from the drop-down list..

Step 6 To select an existing Policy Profile for the WLAN, click on **Select Existing** and choose a **Policy Profile** from the drop-down list..

Authentication Configurations

Set up the authentication configurations and filters for the WLAN depending on the method you have chosen. These include the keys, filters, ACLs, and parameter maps as applicable to the selected authentication method.

Procedure

Step 1 If you have selected **PSK** as the authentication method, configure the following:

a) In the **WLAN > Pre-Shared Key (PSK)** section, select the PSK format. Choose between ASCII and Hexadecimal formats.
b) From the **PSK type** drop-down list, choose if you want the key to be unencrypted or AES encrypted.
c) In the **Pre-Shared Key** field, enter the pass key for the WLAN.

Step 2 If you have selected **Dot1x** as the authentication method, configure the following:

a) In the **WLAN > AAA** tab, configure the AAA server list for the WLAN.
b) Select any of the available AAA servers to add to the WLAN.
c) To add a new AAA server to the list, click on Add New Server and enter the IP address and server-key.
d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.

Step 3 If you have selected **Local Web Authentication** as the authentication method, configure the following:

a) In the **WLAN > Parameter Map** tab, configure the parameter map for the WLAN. A parameter map sets parameters that can be applied to subscriber sessions during authentication.

1. In the **Global Configuration** section, configure the global parameter map.
2. Enter an IPv4 or IPv6 address to configure a virtual IP address for redirecting the clients to the login page of the controller.
3. From the Trustpoint drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.

b) In the **WLAN > Local Users** tab, enter the username in the local database to establish a username-based authentication system.

1. Enter the user name to be saved.
2. From the **Password Encryption** drop-down list, choose if you want the password to be unencrypted or encrypted.
3. In the **Password** field, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters and can contain embedded spaces.
4. Click on the + sign to add the credentials to the database. Add as many user credentials as required.

Step 4 If you have selected **External Web Authentication** as the authentication method, configure the following:

a) In the **WLAN > Parameter Map** tab, configure the parameter map for the WLAN.

1. In the **Global Configuration** section, configure the global parameter map.
2. Enter an IPv4 or IPv6 address to configure the virtual IP address of the external web authentication login page to which the guest users are redirected.
3. From the **Trustpoint** drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.
5. To create a new parameter map, enter the parameter-map name.
6. In the **Redirect URL for login** field, enter the URL of the external server that will host the authentication page for login.
7. In the **Portal IPV4 Address** field, enter the IPv4 address of the external server to send redirects. If the external server uses an IPv6 address, in the **Portal IPV6 Address** field, enter the IPv6 address of the portal to send redirects.

b) In the **WLAN > ACL / URL Filter** tab, configure the ACL rules and the URL filter list.

1. In the **Pre Auth ACL** section, enter the name of the ACL.
2. In the **IP address** field, enter the source IP address and the destination IP address. This will configure the ACL to permit packet transfer from and to the specified IP address. You can add as many IP addresses as required.
3. In the **URL Filter** section, enter a name for the URL Filter list that you are creating.
4. Use the slider to set the list action to **Permit** or **Deny** the URLs.
5. Specify the URLs in the **URLs** box. Enter every URL on a new line.

Step 5 If you have selected Central Web Authentication as the authentication method, configure the following:

a) In the **WLAN > AAA/ACL** tab, configure the AAA server list and ACL for the WLAN.
b) In the **AAA Configuration** section, select any of the available AAA servers to add to the WLAN. This will be the server where the clients will get authenticated.
c) To add a new AAA server to the list, click on **Add New Server** and enter the IP address and server-key.
d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.
e) In the **ACL List** section, enter the name of the ACL. This ACL will contain the rules regarding URLs that can be accessed by the client and should match the name configured on the RADIUS server.

Tags

To configure tags on the WLAN, click on **Tags** from the left panel.

A Tag's property is defined by the policies associated to it. This property is in turn inherited by an associated client/AP. There are various type of tags, each associated to different profiles.

Procedure

Step 1 In the **Site Configuration** section, either enter a site tag to be added, or select an existing site tag from the drop-down list. You can add as many tags as required. In the local mode, the site tag contains the AP join profile only.

Step 2 In the **Policy Tag** section, either enter a policy tag to be added, or select an existing policy tag from the drop-down list. You can add as many tags as required. The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client.

Step 3 In the **RF Tag** section, either enter an RF tag to be added, or select an existing RF tag from the drop-down list. You can add as many tags as required. The RF tag contains the 2.4 GHz and 5 GHz RF profiles.

AP Provisioning

Once the Wireless network and RF characteristics are set up, access points can be added to the local site either using static AP MAC address assignment or by assigning already joined APs to a specific location.

To add tags and associate APs to the WLAN, click on **AP Provisioning** from the left panel.

Procedure

Step 1 The APs already discovered by the controller are listed in the **Provision Joined APs** tab. You can select the APs to be associated to the WLAN from this table.

Step 2 To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.

Step 3 To add APs manually, click on the **Pre-provision APs** tab. You can either add individual MAC addresses of the APs or upload a CSV file with the AP MAC addresses listed. The added APs will be listed in the table below.

Step 4 Select the APs to be associated to the WLAN from this table.

Step 5 To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.

A table of all the APs and the tags added to them is displayed in the **Selected APs** tab.

Step 6 Click **Apply**.

This will create a WLAN in local mode with the authentication method, authentication filters, tags, and APs configured on it.

FlexConnect Mode

FlexConnect is a wireless solution for branch office and remote office deployments. It enables you to configure and control access points (AP) in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic and perform client authentication locally when their connection to the controller is lost. An

AP in Flex mode offers network survivability in the event of a loss of connection to the centralized wireless controller.

Authentication Method

To configure a WLAN for FlexConnect mode, select the preferred authentication method from the left panel. The authentication method sets the method by which a client can access the WLAN and decides the level of security on the WLAN.

The options are:

- Local Web Authentication: The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication.
- External Web Authentication: The controller intercepts htttp(s) traffic and redirects the client to the login page hosted on the external web server for authentication.
- Central Web Authentication: The controller redirects all web traffic from the client to the ISE login page for authentication.

WLAN Profile and Policy

After selecting the Authentication method, click on **WLAN** on the left panel to enter the WLAN profile and policy details.

The WLAN profile defines the properties of a WLAN such as Profile Name, Status, WLAN ID, L2 and L3 Security parameters, AAA Server associated with this SSID and other parameters that are specific to a particular WLAN. The policy profile defines the network policies and the switching policies for a client (with the exception of QoS), which constitute the AP policies as well.

Procedure

Step 1 In the **Network Name** section, enter a **WLAN profile name**, which is a unique name for your wireless network. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 2 Enter a valid **SSID** for the WLAN. A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.

Step 3 Enter the **WLAN ID**.

Step 4 In the **WLAN Policy** section, enter the **Policy Profile name**. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 5 Select the **VLAN** to be associated with the Policy Profile from the drop-down list..

Step 6 To select an existing Policy Profile for the WLAN, click on **Select Existing** and choose a **Policy Profile** from the drop-down list..

Authentication Configurations

Set up the authentication configurations and filters for the WLAN depending on the method you have chosen. These include the keys, filters, ACLs, and parameter maps as applicable to the selected authentication method.

Procedure

Step 1 If you have selected **Local Web Authentication** as the authentication method, configure the following:

a) In the **WLAN > Parameter Map** tab, configure the parameter map for the WLAN. A parameter map sets parameters that can be applied to subscriber sessions during authentication.

1. In the **Global Configuration** section, configure the global parameter map.
2. Enter an IPv4 or IPv6 address to configure a virtual IP address for redirecting the clients to the login page of the controller.
3. From the **Trustpoint** drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.

b) In the WLAN > Local Users / Flex tab, configure a Flex profile and enter the username in the local database to establish a username-based authentication system.

1. In the **Flex Profile** section, enter the name of the new flex profile and the native VLAN ID.
2. To use an already existing Flex profile, click on **Select Existing** to choose a profile from the drop-down list and enter the native VLAN ID.
3. In the **Local Users** section, enter the user name to be saved.
4. From the **Password Encryption** drop-down list, choose if you want the password to be unencrypted or encrypted.
5. In the **Password** field, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters and can contain embedded spaces.
6. Click on the + sign to add the credentials to the database. Add as many user credentials as required.

Step 2 If you have selected **External Web Authentication** as the authentication method, configure the following:

a) In the **WLAN > Parameter Map** tab, configure the parameter map for the WLAN.

1. In the **Global Configuration** section, configure the global parameter map.
2. Enter an IPv4 or IPv6 address to configure the virtual IP address of the external web authentication login page to which the guest users are redirected.
3. From the **Trustpoint** drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.

5. To create a new parameter map, enter the parameter-map name.
6. In the **Redirect URL for login** field, enter the URL of the external server that will host the authentication page for login.
7. In the **Portal IPV4 Address** field, enter the IPv4 address of the external server to send redirects. If the external server uses an IPv6 address, in the **Portal IPV6 Address** field, enter the IPv6 address of the portal to send redirects.

b) In the **WLAN > ACL / URL Filter** tab, configure the ACL rules and the URL filter list.

1. In the **Flex Profile** section, enter the name of the new flex profile and the native VLAN ID.
2. To use an already existing Flex profile, click on **Select Existing** to choose a profile from the drop-down list and enter the native VLAN ID.
3. In the **Pre Auth ACL** section, enter the name of the ACL.
4. In the **IP address** field, enter the source IP address and the destination IP address. This will configure the ACL to permit packet transfer from and to the specified IP address. You can add as many IP addresses as required.
5. In the **URL Filter** section, enter a name for the URL Filter list that you are creating.
6. Click on **Add** to add the URLs.
7. Specify the URL to be added to the list and its preference.
8. Use the slider to set the list action to **Permit** or **Deny** the URLs.
9. Click **Save**.

   You can add as many URLs to the list as required.

c) To add a new AAA server to the list, click on Add New Server and enter the IP address and server-key.
d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.

Step 3 If you have selected **Central Web Authentication** as the authentication method, configure the following:

a) In the **WLAN > AAA/ACL** tab, configure the AAA server list and ACL for the WLAN.
b) In the **AAA Configuration** section, select any of the available AAA servers to add to the WLAN. This will be the server where the clients will get authenticated.
c) To add a new AAA server to the list, click on **Add New Server** and enter the IP address and server-key.
d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.
e) In the **Flex Profile** section, enter the name of the new flex profile and the native VLAN ID.
f) To use an already existing Flex profile, click on **Select Existing** to choose a profile from the drop-down list and enter the native VLAN ID.
g) In the **ACL List** section, enter the name of the ACL. This ACL will contain the rules regarding URLs that can be accessed by the client and should match the name configured on the RADIUS server.

Tags

To configure tags on the WLAN, click on **Tags** from the left panel.

A Tag's property is defined by the policies associated to it. This property is in turn inherited by an associated client/AP. There are various type of tags, each associated to different profiles.

Procedure

Step 1 In the **Site Configuration** section, either enter a site tag to be added, or select an existing site tag from the drop-down list. You can add as many tags as required. In FlexConnect mode, the site tag contains the AP join profile and the Flex profile.

Step 2 In the **Policy Tag** section, either enter a policy tag to be added, or select an existing policy tag from the drop-down list. You can add as many tags as required. The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client.

Step 3 In the **RF Tag** section, either enter an RF tag to be added, or select an existing RF tag from the drop-down list. You can add as many tags as required. The RF tag contains the 2.4 GHz and 5 GHz RF profiles.

AP Provisioning

Once the Wireless network and RF characteristics are set up, access points can be added to the local site either using static AP MAC address assignment or by assigning already joined APs to a specific location.

To add tags and associate APs to the WLAN, click on **AP Provisioning** from the left panel.

Procedure

Step 1 The APs already discovered by the controller are listed in the **Provision Joined APs** tab. You can select the APs to be associated to the WLAN from this table.

Step 2 To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.

Step 3 To add APs manually, click on the **Pre-provision APs** tab. You can either add individual MAC addresses of the APs or upload a CSV file with the AP MAC addresses listed. The added APs will be listed in the table below.

Step 4 Select the APs to be associated to the WLAN from this table.

Step 5 To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.

A table of all the APs and the tags added to them is displayed in the **Selected APs** tab.

Step 6 Click **Apply**.

This will create a WLAN in FlexConnect mode with the authentication method, authentication filters, tags, and APs configured on it.

Guest CWA Mode

The Guest mode addresses the need to provide internet access to guests in a secure and accountable manner with Central Web Authentication as the security method. The implementation of a wireless guest network

uses the enterprise's existing wireless and wired infrastructure to the maximum extent. This solution comprises of two controllers - a Guest Foreign and a Guest Anchor.

Controller Type

To configure a WLAN for Guest CWA mode, select the type of controller configuration you want to set up on the device from the left panel.

The options are:

- Foreign: A Foreign is a controller in the WLAN that exists in the enterprise. A client sends a connection request to a Foreign controller to join the WLAN. It is a dedicated guest WLAN or SSID and is implemented throughout the campus wireless network wherever guest access is required. The Foreign controller manages the anchor controllers.
- Anchor: An Anchor is a controller or group of controllers in a WLAN that manage traffic within the network for a guest client. It provides internal security by forwarding the traffic from a guest client to a Cisco Wireless Controller in the demilitarized zone (DMZ) network.

WLAN Profile and Policy

After selecting the Authentication method, click on **WLAN** on the left panel to enter the WLAN profile and policy details.

The WLAN profile defines the properties of a WLAN such as Profile Name, Status, WLAN ID, L2 and L3 Security parameters, AAA Server associated with this SSID and other parameters that are specific to a particular WLAN. The policy profile defines the network policies and the switching policies for a client (with the exception of QoS), which constitute the AP policies as well.

Procedure

Step 1 In the **Network Name** section, enter a **WLAN profile name**, which is a unique name for your wireless network. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 2 Enter a valid **SSID** for the WLAN. A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.

Step 3 Enter the **WLAN ID**.

Step 4 In the **WLAN Policy** section, enter the **Policy Profile name**. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 5 Select the **VLAN** to be associated with the Policy Profile from the drop-down list..

Step 6 To select an existing Policy Profile for the WLAN, click on **Select Existing** and choose a **Policy Profile** from the drop-down list..

Step 7 If you have selected **Foreign**, in the **Mobility Anchors** section, select the IP address of an available controller to assign it as the mobility anchor for the WLAN. This will extend the configurations on the Foreign controller onto the anchor controllers as well.

Authentication Configurations

For the Guest access mode, the authentication method is Central Web Authentication.

Procedure

Step 1 In the **WLAN > AAA/ACL** tab, configure the AAA server list and ACL for the WLAN.

Step 2 In the **AAA Configuration** section, select any of the available AAA servers to add to the WLAN. This will be the server where the clients will get authenticated.

Step 3 To add a new AAA server to the list, click on **Add New Server** and enter the IP address and server-key.

Step 4 To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.

Step 5 In the **ACL List** section, enter the name of the ACL. This ACL will contain the rules regarding URLs that can be accessed by the client and should match the name configured on the RADIUS server.

Tags

To configure tags on the WLAN, click on **Tags** from the left panel.

A Tag's property is defined by the policies associated to it. This property is in turn inherited by an associated client/AP. There are various type of tags, each associated to different profiles.

Procedure

Step 1 In the **Site Configuration** section, either enter a site tag to be added, or select an existing site tag from the drop-down list. You can add as many tags as required.

Step 2 In the **Policy Tag** section, either enter a policy tag to be added, or select an existing policy tag from the drop-down list. You can add as many tags as required. The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client.

Step 3 In the **RF Tag** section, either enter an RF tag to be added, or select an existing RF tag from the drop-down list. You can add as many tags as required. The RF tag contains the 2.4 GHz and 5 GHz RF profiles.

AP Provisioning

Once the Wireless network and RF characteristics are set up, access points can be added to the local site either using static AP MAC address assignment or by assigning already joined APs to a specific location.

If you have selected **Foreign**, click on **AP Provisioning** from the left panel to add tags and associate APs to the WLAN.

Procedure

Step 1 The APs already discovered by the controller are listed in the **Provision Joined APs** tab. You can select the APs to be associated to the WLAN from this table.

Step 2 To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.

Step 3 To add APs manually, click on the **Pre-provision APs** tab. You can either add individual MAC addresses of the APs or upload a CSV file with the AP MAC addresses listed. The added APs will be listed in the table below.

Step 4 Select the APs to be associated to the WLAN from this table.

Step 5 To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.

A table of all the APs and the tags added to them is displayed in the **Selected APs** tab.

Step 6 Click **Apply**.

This will create a WLAN in Guest CWA mode with the authentication method, mobility anchors, authentication filters, tags, and APs configured on it.

Creating WLANs (GUI)

Procedure

Step 1 In the **Configuration** > **Tags & Profiles** > **WLANs** page, click **Add**.

The **Add WLAN** window is displayed.

Step 2 Under the **General** tab and **Profile Name** field, enter the name of the WLAN. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 3 Click **Save & Apply to Device**.

Creating WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*]	Specifies the WLAN name and ID:

	Command or Action	Purpose
	Example: `Device(config)# wlan mywlan 34 mywlan-ssid`	• For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters. • For the *wlan-id*, enter the WLAN ID. The range is from 1 to 512. • For the *ssid*, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** • You can create SSID using GUI or CLI. However, we recommend that you use CLI to create SSID. • By default, the WLAN is disabled.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Deleting WLANs (GUI)

Procedure

Step 1 In the **Configuration** > **Tags & Profiles** > **WLANs** page, check the checkbox adjacent to the WLAN you want to delete.

To delete multiple WLANs, select multiple WLANs checkboxes.

Step 2 Click **Delete**.

Step 3 Click **Yes** on the confirmation window to delete the WLAN.

Deleting WLANs

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**no wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# no wlan test2`	Deletes the WLAN. The arguments are as follows: • The *wlan-name* is the WLAN profile name. • The *wlan-id* is the WLAN ID. • The *ssid* is the WLAN SSID name configured for the WLAN. **Note** If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Searching WLANs (CLI)

To verify the list of all WLANs configured on the controller, use the following show command:

```
Device# show wlan summary
Number of WLANs: 4

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
1    test1                             test1-ssid                     137  UP
3    test2                             test2-ssid                     136  UP
2    test3                             test3-ssid                     1    UP
45   test4                             test4-ssid                     1    DOWN
```

To use wild cards and search for WLANs, use the following `show` command:

```
Device# show wlan summary | include test-wlan-ssid
1    test-wlan                        test-wlan-ssid                   137   UP
```

Enabling WLANs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the WLAN name.

Step 3 In the **Edit WLAN** window, toggle the **Status** button to **ENABLED**.

Step 4 Click **Update & Apply to Device**.

Enabling WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Disabling WLANs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 In the **WLANs** window, click the WLAN name.

Step 3 In the **Edit WLAN** window, set the **Status** toggle button as **DISABLED**.

Step 4 Click **Update & Apply to Device**.

Disabling WLANs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.
Step 5	**show wlan summary** **Example:** `Device# show wlan summary`	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Radio

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 4	**broadcast-ssid** **Example:**	Broadcasts the SSID for this WLAN.

	Command or Action	Purpose
	`Device(config-wlan)# broadcast-ssid`	
Step 5	**dot11bg 11g** **Example:** `Device(config-wlan)# dot11bg 11g`	Configures the WLAN radio policy for dot11 radios. Also see the section: Configuring a WLAN Radio Policy.
Step 6	**media-stream multicast-direct** **Example:** `Device(config-wlan)# media-stream multicast-direct`	Enables multicast VLANs on this WLAN.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 8	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Advanced WLAN Properties (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**chd** **Example:** `Device(config-wlan)# chd`	Enables coverage hole detection for this WLAN.
Step 4	**ccx aironet-iesupport** **Example:** `Device(config-wlan)# ccx aironet-iesupport`	Enables support for Aironet IEs for this WLAN.

	Command or Action	Purpose
Step 5	**client association limit** {*clients-per-wlan* | **ap** *clients-per-ap-per-wlan* | **radio***clients-per-ap-radio--per-wlan*} **Example:** `Device(config-wlan)# client association limit ap 400`	Sets the maximum number of clients, clients per AP, or clients per AP radio that can be configured on a WLAN.
Step 6	**ip access-group web** *acl-name* **Example:** `Device(config-wlan)# ip access-group web test-acl-name`	Configures the IPv4 WLAN web ACL. The variable *acl-name* specifies the user-defined IPv4 ACL name.
Step 7	**peer-blocking** [**allow-private-group** | **drop** | **forward-upstream**] **Example:** `Device(config-wlan)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **allow-private-group**—Enables peer-to-peer blocking on the Allow Private Group action. • **drop**—Enables peer-to-peer blocking on the drop action. • **forward-upstream**—No action is taken and forwards packets to the upstream. **Note** The **forward-upstream** option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP.
Step 8	**channel-scan** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} **Example:** `Device(config-wlan)# channel-scan defer-priority 6`	Sets the channel scan defer priority and defer time. The arguments are as follows: • **defer-priority**—Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3. • **defer-time**—Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Configuring Advanced WLAN Properties (GUI)

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs** .

Step 2 Click **Add**.

Step 3 Under the **Advanced** tab, check the **Coverage Hole Detection** check box.

Step 4 Check the **Aironet IE** check box to enable Aironet IE on the WLAN.

Step 5 Check the **Diagnostic Channel** check box to enable diagnostic channel on the WLAN.

Step 6 From the **P2P Blocking Action** drop-down list, choose the required value.

Step 7 Set the **Multicast Buffer** toggle button as enabled or diabled.

Step 8 Check the **Media Stream Multicast-Direct** check box to enable the feature.

Step 9 In the **Max Client Connections** section, specify the maximum number of client connections for the following:

- In the **Per WLAN** field, enter a value. The valid range is between 0 and 10000.
- In the **Per AP Per WLAN** field, enter a value. The valid range is between 0 and 400.
- In the **Per AP Radio Per WLAN** field, enter a value. The valid range is between 0 and 200.

Step 10 In the **11v BSS Transition Support** section, perform the following configuration tasks:

a) Check the BSS Transition check box to enable 802.11v BSS Transition support.
b) In the **Disassociation Imminent** field, enter a value. The valid range is between 0 and 3000.
c) In the **Optimized Roaming Disassociation Timer** field, enter a value. The valid range is between 0 and 40.
d) Select the check box to enable the following:

- BSS Max Idle Service
- BSS Max Idle Protected
- Disassociation Imminent Service
- Directed Multicast Service
- Universal Admin
- Load Balance
- Band Select
- IP Source Guard

Step 11 In the 11ax section, perform the following configuration tasks:

a) Select the check box to enable the following:

- Check the **Enable 11ax** checkbox to enable 802.11ax operation status on the WLAN.

- Check the **Downlink OFDMA** and **Uplink OFDMA** check boxes to enable downlink and uplink connections that use OFDMA.

  Orthogonal Frequency Division Multiple Access (OFDMA) is a channel access mechanism that assures contention-free transmission to multiple clients in both the downlink (DL) and uplink (UL) within a respective single transmit opportunity.

- Check the **Downlink MU-MIMO** and **Uplink MU-MIMO** check boxes to enable downlink and uplink connections that use MU-MIMO.

  With Multiuser MIMO (MU-MIMO), an AP can use its antenna resources to transmit multiple frames to different clients, all at the same time and over the same frequency spectrum.

- Enable the target wake up time configuration on the WLAN by checking the **BSS Target Wake Up Time** checkbox.

  Target wake up time allows an AP to manage activity in the Wi-Fi network to minimize medium contention between stations, and to reduce the required amount of time that a station in the power-save mode needs to be awake. This is achieved by allocating stations to operate at non-overlapping times, and/or frequencies, and concentrate the frame exchanges in predefined service periods.

- Check the **Universal Admin** check box to enable Universal Admin support for the WLAN.

- Enable OKC on the WLAN by checking the **OKC** check box. Opportunistic Key Caching (OKC) allows the wireless client and the WLAN infrastructure to cache only one Pairwise Master Key (PMK) for the lifetime of the client association with this WLAN, even when roaming between multiple APs. This is enabled by default.

- Check the **Load Balance** check box to enable Aggressive Client Load Balancing. This allows lightweight access points to load balance wireless clients across access points.

- Check the **Band Select** check box to enable band selection for the WLAN. Band selection enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested with interference from other electronic devices as well as co-channel interference from other access points. Band selection helps prevent these sources of interference and improve overall network performance.

- Enable IP Source Guard on the WLAN by checking the **IP Source Guard** check box. IP Source Guard (IPSG) is a Layer 2 security feature that prevents the wireless controller from forwarding the packets with source IP addresses that are not known to it.

b) From the **WMM Policy** drop-down list, choose the policy as **Allowed**, **Disabled**, or **Required**. By default, the WMM policy is **Allowed**. Wi-Fi Multimedia (WMM) is used to prioritize different types of traffic.

- **Disabled**: Disables WMM on the WLAN.

- **Required**: Requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

- **Allowed**: Devices that cannot support WMM can join the WLAN but will not benefit from the 802.11n rates.

c) From the **mDNS** drop-down list, choose **Bridging**, **Gateway**, or **Drop**. Multicast DNS (mDNS) provides the ability to perform DNS-like operations on the local link in the absence of any conventional Unicast DNS server.

- **Bridging**: Packets with mDNS multicast IP and multicast mac will be sent on multicast CAPWAP tunnel.
- **Gateway**: All ingress mDNS packets received from the wired network on a L3 interface (SVI or physical) would be intercepted by the Controller software and processed.
- **Drop**: All ingress mDNS packets will be dropped.

Step 12 In the **Off Channel Scanning Defer** section, choose the appropriate **Defer Priority** values and then specify the required Scan Defer Time value in milliseconds.

Step 13 In the **Assisted Roaming (11k)** section, choose the appropriate status for the following:

- Prediction Optimization
- Neighbor List
- Dual-Band Neighbor List

Step 14 In the **DTIM Period (in beacon intervals)** section, specify a value for 802.11a/n and 802.11b/g/n radios. The valid range is from 1 to 255.

Step 15 Click **Apply to Device**.

Configuring WLAN Radio Policy (GUI)

Procedure

Step 1 On the **Configuration** > **Tags & Profiles** > **WLANs** page, click **Add** to create WLANs.

Step 2 In the **General** tab, enter a **Profile Name**, which is a unique name of the your wireless network.

The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 3 Enter a valid **SSID** for the WLAN.

A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.

Step 4 Enter the **WLAN ID**. The valid range for the different models are listed below:

Model	WLAN ID Range
Cisco Catalyst 9800-80 Wireless Controller	1-4096
Cisco Catalyst 9800-CL Wireless Controller	1-4096
Cisco Catalyst 9800-40 Wireless Controller	1-4096
Cisco Catalyst 9800-L Wireless Controller	1-4096
Cisco Embedded Wireless Controller for an AP	1-16

Step 5 Set the WLAN **Status** to Enabled.

Step 6 To broadcast the SSID of the WLAN, set the status of Broadcast SSID to enabled. By default, this is disabled.

Step 7 In the **Radio Policy** section, enable the desired radio band for the WLAN.

- 2.4ghz – Configures the policy on the 2.4-GHz radio.
- 5ghz – Configures the policy on the 5-GHz radio.

Step 8 If you enable the 5ghz radio band, select the radio slot to broadcast the WLAN on. The options are slot 0, slot 1, and slot 2. You can select multiple slots for the WLAN.

Step 9 From the 802.11b/g Policy drop-down list, choose the radio policy from the following options:

- 802.11g only
- 802.11b/g

Click **Apply to Device**.

Configuring a WLAN Radio Policy (CLI)

Configure WLAN radio policy using commands.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**shutdown** **Example:** `Device(config-wlan)# shutdown`	Disables the WLAN.
Step 4	**radio policy dot11** {**5ghz** | **24ghz** | **6ghz** } **Example:** `Device(config-wlan)# radio policy dot11 5ghz`	Enables the corresponding radio policy on the WLAN. The options are: • **2.4ghz**: Configures the WLAN on 2.4-GHz radio only. • **5ghz**: Configures the WLAN on 5-GHz radio only. • **6ghz**: Configures the WLAN on 6-GHz radio only.

	Command or Action	Purpose
Step 5	**slot {0| 1 | 2}** **Example:** `Device(config-wlan-radio-5ghz)# slot 1`	Configures the WLAN radio policy on the slot that you choose. The options are: • **0**: Configures the WLAN on the 5GHz radio with radio slot 0 (if using 5GHz). • **1**: Configures the WLAN on the 5GHz radio with radio slot 1. • **2**: Configures the WLAN on the 5GHz radio with radio slot 2 (if present).
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 7	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode.

Verifying WLAN Properties (CLI)

To verify the WLAN properties based on the WLAN ID, use the following `show` command:

```
Device# show wlan id wlan-id
```

To verify the WLAN properties based on the WLAN name, use the following `show` command:

```
Device# show wlan name wlan-name
```

To verify the WLAN properties of all the configured WLANs, use the following `show` command:

```
Device# show wlan all
```

To verify the summary of all WLANs, use the following `show` command:

```
Device# show wlan summary
```

To verify the running configuration of a WLAN based on the WLAN name, use the following `show` command:

```
Device# show running-config wlan wlan-name
```

To verify the running configuration of all WLANs, use the following `show` command:

```
Device# show running-config wlan
```

Verifying WLAN-VLAN Information for an AP

To verify the operational WLAN-VLAN mappings per AP, use the following command:

```
Device# show ap name test wlan vlan

Policy tag mapping
```

```
------------------
WLAN Profile Name Name Policy    VLAN   Flex Central Switching  IPv4 ACL    IPv6 ACL
-----------------------------------------------------------------------------------------
jey_cwa           pp-local-1     46       Enabled               jey_acl1   Not Configured
swaguest          pp-local-1     46       Enabled               jey_acl1   Not Configured
```

Verifying a WLAN Radio Policy

To verify the WLAN radio policy configuration status, use the following command:

```
Device# show wlan id 6 | sec Radio Bands
wpa3 enabled wlan:
Configured Radio Bands: All
Operational State of Radio Bands : All Bands Operational

Configured Radio Bands : All
Operational State of Radio Bands
    2.4ghz                      : UP
    5ghz                        : UP
    6ghz                        : DOWN (Required config: Disable WPA2 and Enable WPA3 &
dot11ax)

wpa3 not enabled wlan :
Configured Radio Bands : All
Operational State of Radio Bands
2.4ghz : UP
5ghz   : UP

5ghz specify slot is enabled :
Configured Radio Bands
5ghz   : Enabled
Slot 0 : Enabled
Slot 1 : Disabled
Slot 2 : Disabled

Operational State of Radio Bands
5ghz   : UP
Slot 0 : Enabled
Slot 1 : Disabled
Slot 2 : Disabled
```

CHAPTER 167

WLAN Security

- Information About WPA1 and WPA2, on page 1871
- Information About AAA Override, on page 1872
- Prerequisites for Layer 2 Security, on page 1875
- Restrictions for WPA2 and WP3, on page 1876
- Feature History for Fallback for AAA-Overridden VLAN, on page 1876
- Information About Fallback for AAA- Overridden VLAN, on page 1877
- Configuring Fallback for AAA-Overridden VLAN (CLI), on page 1878
- Verifying Fallback for AAA-Overridden VLAN, on page 1878
- How to Configure WLAN Security, on page 1879

Information About WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and Message Integrity Check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). By default, both WPA1 and WPA2 use the 802.1X for authenticated key management. However, the following options are also available:

- PSK—When you choose PSK (also known as WPA preshared key or WPA passphrase), you need to configure a preshared key (or a passphrase). This key is used as the Pairwise Master Key (PMK) between clients and authentication server.
- Cisco Centralized Key Management uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller , typically in under 150 milliseconds (ms). Cisco Centralized Key Management reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. Cisco Centralized Key Management fast secure roaming ensures that there is no perceptible delay in time-sensitive applications, such as wireless Voice over IP (VoIP), Enterprise Resource Planning (ERP), or Citrix-based solutions. Cisco Centralized Key Management is a CCXv4-compliant feature. If Cisco Centralized Key Management is selected, only Cisco Centralized Key Management clients are supported.

When Cisco Centralized Key Management is enabled, the behavior of access points differs from the controller 's for fast roaming in the following ways:

- If an association request sent by a client has Cisco Centralized Key Management enabled in a Robust Secure Network Information Element (RSN IE) but Cisco Centralized Key Management IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.
- If an association request sent by a client has Cisco Centralized Key Management enabled in RSN IE and Cisco Centralized Key Management IE is encoded and only PMKID is present in the RSN IE, then the AP does a full authentication. The access point does not use PMKID sent with the association request when Cisco Centralized Key Management is enabled in RSN IE.

- 802.1X+Cisco Centralized Key Management—During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and Cisco Centralized Key Management fast secure roaming, Cisco Centralized Key Management-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+Cisco Centralized Key Management is considered as an optional Cisco Centralized Key Management because both Cisco Centralized Key Management and non-Cisco Centralized Key Management clients are supported when this option is selected.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/Cisco Centralized Key Management/802.1X+Cisco Centralized Key Management clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/Cisco Centralized Key Management/ 802.1X+Cisco Centralized Key Management information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two ciphers, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

Information About AAA Override

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Configuring AAA Override

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:**	Configures WLAN policy profile and enters the wireless policy configuration mode.

	Command or Action	Purpose
	`Device(config)# wireless profile policy test-wgb`	
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA policy override. **Note** If VLAN is not pushed from the RADIUS server, the VLAN Override feature can be disabled from the RADIUS server.
Step 4	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Information About VLAN Override

The VLAN override requires the AAA Override to be enabled under the Policy Profile.

You can assign VLAN from the RADIUS server in two ways:

- Using IEFT RADIUS attributes 64, 65, and 81—The attribute 81 can be a VLAN ID, VLAN name, or VLAN group name. Both VLAN name and VLAN group are supported. Therefore, VLAN ID does not need to be predetermined on RADIUS.

  The RADIUS user attributes used for the VLAN ID assignment are:

  - 64 (Tunnel-Type)—Must be set to VLAN (Integer = 13).
  - 65 (Tunnel-Medium-Type)—Must be set to 802 (Integer = 6).
  - 81 (Tunnel-Private-Group-ID)—Must be set to the corresponding VLAN ID, VLAN name, or VLAN group name.

- Using Aire-Interface-Name attribute—Use this attribute to assign a successfully authenticated user to a VLAN interface name (or VLAN ID) as per the user configuration. When you use this attribute, the VLAN name is returned as a string.

The VLAN ID is 12-bits, and takes a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type string, as defined in RFC2868 for use with IEEE 802.1X, the VLAN ID integer value is encoded as a string. When these tunnel attributes are sent, it is necessary to fill in the Tag field.

Configuring Override VLAN for Central Switching

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**vlan** *vlan-id* **Example:** `Device(config)# vlan 20`	Defines VLANs that can be pushed from the RADIUS server. **Note** The valid VLAN ID ranges from 1 to 4094.
Step 3	**name** *vlan-name* **Example:** `Device(config-vlan)# name vlan_ascii`	(Optional) Changes the default name of the VLAN.
Step 4	**end** **Example:** `Device(config-vlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Override VLAN for Local Switching

If the VLAN name ID mapping under flex profile is newly added or updated, then the WLAN policy profiles having a matching VLAN name configured, must be shut and unshut. This is to ensure that the updated WLAN-VLAN mapping is pushed to the APs and the client receives the IP address from the intended VLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex_profile_name* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a Flex profile.
Step 3	**vlan-name** *vlan_name* **Example:** `Device(config-wireless-flex-profile)# vlan-name vlan_123`	Defines VLANs that can be pushed from the RADIUS server.
Step 4	**vlan-id** *vlan_id* **Example:** `Device(config-wireless-flex-profile-vlan)# vlan-id 23`	Configures VLAN ID. The valid VLAN ID ranges from 1 to 4096.
Step 5	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-wireless-flex-profile-vlan)# end`	Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

VLAN Override on Layer 3 Web Authentication

The VLAN override can be pushed from the RADIUS server during Layer 3 authentication.

When a client gets connected to the controller and authenticated using the RADIUS server for Local Web Authentication (LWA) and Central Web Authentication (CWA), the RADIUS server pushes back in access-accept the new VLAN. If the RADIUS server pushes back a new VLAN in the access-accept, the client goes back to IP learn state on the controller. The controller de-associates the client while maintaining the client state for 30 seconds. Once the client re-associates, the client lands immediately to the new VLAN and re-triggers a new DHCP request. The client then learns a new IP and moves to the RUN state on the controller.

The VLAN Override on Layer 3 Web authentication supports the following:

- Local clients
- Anchored clients
- FlexConnect central authentication, central or local switching

Verifying VLAN Override on Layer 3 Web Authentication

To display the VLAN override after L3 authentication, use the following command:

```
Device# show wireless client mac <mac> detail
[…]
        Vlan Override after L3 Auth: True
```

To display the statistics about client, use the following command:

```
Device# show wireless stats client detail
[…]
      Total L3 VLAN Override vlan change received      : 1
      Total L3 VLAN Override disassociations sent      : 1
      Total L3 VLAN Override re-associations received  : 1
      Total L3 VLAN Override successful VLAN change    : 1
      […]
      L3 VLAN Override connection timeout                          : 0
```

Prerequisites for Layer 2 Security

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on the information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- WPA+WPA2

Note

- Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.
- A WLAN configured with TKIP support will not be enabled on an RM3000AC module.

- Static WEP (not supported on Wave 2 APs)

Restrictions for WPA2 and WP3

- You cannot enable security ft or ft-adaptive without enabling WPA2 or WPA3.
- You cannot enable ft-dot1x or ft-psk without enabling WPA2 or WPA3.
- You cannot enable 802.1x or PSK simultaneously with SHA256 key derivation type without enabling WPA2 or WPA3 on a WLAN.
- You cannot configure PMF on WPA1 WLAN without WPA2 security.
- IOS APs do not support WPA3.

Feature History for Fallback for AAA-Overridden VLAN

This table provides release and related information for the feature explained in this module.

This feature is available in all the releases subsequent to the one in which it is introduced in, unless noted otherwise.

Table 136: Feature History for Fallback for AAA-Overridden VLAN

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.6.1	Fallback for AAA-Overridden VLAN	In Cisco IOS XE Bengaluru 17.5.1 and earlier releases, if there is a network with a single AAA server dictating policies that need to be applied to a client; and this client moves across different sites that have different policy definitions. If these policy definitions are not defined on the site to which the client needs to connect, the client does not get access to the network. For example, if a client is to be given access in VLAN 1, and VLAN 1 is not defined on the site to which the client connects, the client is excluded and does not get any access to the network. The Fallback for AAA-Overridden VLAN feature is introduced to allow fallback to policy profile VLAN when the overridden VLAN is not available.

Information About Fallback for AAA- Overridden VLAN

From Cisco IOS XE Bengaluru 17.6.1, fallback for AAA-overridden VLAN or VLAN groups is supported on the wireless policy profile.

A new command is introduced in the wireless policy profile to configure the Fallback for AAA-Overridden VLAN feature. In Cisco IOS XE Bengaluru 17.6.1, you cannot configure the Fallback for AAA Overridden VLAN feature using the GUI.

Central Switching and FlexConnect Mode Scenarios

If fallback is enabled for AAA-overridden VLAN or VLAN groups, you might encounter the following scenarios in Central Switching and FlexConnect modes.

Central Switching:

If the AAA server gives a VLAN policy to a client, and the VLAN ID or the VLAN name is defined in the controller, the client is assigned to the VLAN specified by the AAA server. If the VLAN is not defined in the controller, the client is assigned to a VLAN that is configured on the wireless policy profile.

If a VLAN group is configured on a wireless policy profile, the VLAN, as computed by the existing VLAN group logic, is assigned to the client. In the VLAN group case, fallback to policy profile VLAN occurs only when all the VLANs in the group are not configured in the controller, or, if the VLAN group is not defined in the controller.

If both, AAA-overridden VLAN and the VLAN configured on the wireless policy profile are not defined in the controller, the configuration is termed as invalid, and the client is excluded.

If a VLAN policy is not configured, or, if the default wireless policy profile is configured, the client is assigned a VLAN from the management VLAN.

FlexConnect Mode:

If the AAA server assigns a VLAN policy to a client configured in the FlexConnect profile, the VLAN is resolved by the controller. If the VLAN is not configured on the FlexConnect profile, the behavior of the

VLAN name and the VLAN ID is made consistent, with the help of the fallback feature, and the client receives the IP address from the wireless policy profile configuration.

The following points summarize the FlexConnect mode behavior:

- If AAA VLAN is defined in FlexConnect profile, the client is assigned the AAA VLAN.
- If AAA VLAN is not defined in the FlexConnect profile, FlexConnect VLAN Central Switching is configured, and VLAN is defined in the controller, and the client is assigned AAA VLAN and is centrally switched.
- If AAA VLAN is not defined in the FlexConnect profile, FlexConnect VLAN Central Switching is configured, the VLAN is not defined in the controller, and the client is assigned a VLAN from the wireless policy profile.
- If AAA VLAN is not defined in the FlexConnect profile, and FlexConnect VLAN Central Switching is not configured, the client is assigned a VLAN from the wireless policy profile.

Configuring Fallback for AAA-Overridden VLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)# wireless profile policy wlan-policy-profile-name`	Configures the WLAN policy profile. Enters the wireless policy profile configuration mode.
Step 3	**aaa-override vlan fallback** **Example:** `Device(config-wireless-policy)# aaa-override vlan fallback`	Allows fallback to the policy profile VLAN when the overridden VLAN is not available.

Verifying Fallback for AAA-Overridden VLAN

To verify if the fallback for AAA-overridden VLAN is enabled, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile | sec AAA Policy Params
AAA Policy Params
  AAA Override                  : DISABLED
  NAC                           : DISABLED
  AAA Policy name               : default-aaa-policy
  AAA Vlan Fallback             : ENABLED
```

How to Configure WLAN Security

Configuring Static WEP Layer 2 Security Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the name of the WLAN.

Step 3 In the **Edit WLAN** window, click the **Security** tab.

Step 4 From the **Layer 2 Security Mode** drop-down list, select the **Static WEP** option.

Step 5 (Optional) Check the **Shared Key Authentication** check box to set the authentication type as shared. By leaving the check box unchecked, the authentication type is set to open.

Step 6 Set the **Key Size** as either **40 bits** or **104 bits**.

- 40 bits: The keys with 40-bit encryption must contain 5 ASCII text characters or 10 hexadecimal characters.
- 104 bits: The keys with 104-bit encryption must contain 13 ASCII text characters or 26 hexadecimal characters.

Step 7 Set the appropriate **Key Index**; you can choose between 1 to 4.

Step 8 Set the **Key Format** as either **ASCII** or **Hex**.

Step 9 Enter a valid **Encryption Key**.

- 40 bits: The keys with 40-bit encryption must contain 5 ASCII text characters or 10 hexadecimal characters.
- 104 bits: The keys with 104-bit encryption must contain 13 ASCII text characters or 26 hexadecimal characters.

Step 10 Click **Update & Apply to Device**.

Configuring Static WEP Layer 2 Security Parameters (CLI)

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device# wlan test4 1 test4`	Enters the WLAN configuration submode. *profile-name* is the profile name of the configured WLAN. *wlan-id* is the wireless LAN identifier. The range is 1 to 512. *SSID_Name* is the SSID which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 4	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r Fast Transition on the WLAN.
Step 5	**no security wpa**{**akm** | **wpa1** | **wpa2**} **Example:** `Device(config-wlan)# no security wpa wpa1 ciphers tkip`	Disables the WPA/WPA2 support for a WLAN.
Step 6	**security static-wep-key** [**authentication** {**open** | **shared**}] **Example:** `Device(config-wlan)# security static-wep-key authentication open`	The keywords are as follows: • **static-wep-key**—Configures Static WEP Key authentication. • **authentication**—Specifies the authentication type you can set. The values are open and shared.
Step 7	**security static-wep-key** [**encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]] **Example:** `Device(config-wlan)# security static-wep-key encryption 104 ascii 0 1234567890123 1`	The keywords are as follows: • **static-wep-key**—Configures Static WEP Key authentication. • **encryption**—Specifies the encryption type that you can set. The valid values are 104 and 40. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters. • **ascii**—Specifies the key format as ASCII.

	Command or Action	Purpose
		• **hex**—Specifies the key format as HEX.
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring WPA + WPA2 Layer 2 Security Parameters (GUI)

Procedure

Step 1 Click **Configuration** > **Tags and Profiles** > **WLANs**.

Step 2 Click **Add** to add a new WLAN Profile or click the one you want to edit.

Step 3 In the **Edit WLAN** window, click **Security** > **Layer2**.

Step 4 From **Layer 2 Security Mode** drop-down menu, select **WPA + WPA2**.

Step 5 Configure the security parameters and then click **Save and Apply to Device**.

Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

Note The default values for security policy WPA2 are:

- Encryption is AES.
- Authentication Key Management (AKM) is dot1x.

Before you begin

You must have administrator privileges.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device# wlan test4 1 test4`	Enters the WLAN configuration submode. • *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
		• *wlan-id* is the wireless LAN identifier. The range is 1 to 512. • *SSID_Name* is the SSID that contains 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *profile-name* command.
Step 3	**security wpa {akm | wpa1 | wpa2}** **Example:** `Device(config-wlan)# security wpa`	Enables WPA or WPA2 support for WLAN.
Step 4	**security wpa wpa1** **Example:** `Device(config-wlan)# security wpa wpa1`	Enables WPA.
Step 5	**security wpa wpa1 ciphers** [**aes** | **tkip**] **Example:** `Device(config-wlan)# security wpa wpa1 ciphers aes`	Specifies the WPA1 cipher. Choose one of the following encryption types: • **aes**—Specifies WPA/AES support. • **tkip**—Specifies WPA/TKIP support. The default values are TKIP for WPA1 and AES for WPA2. **Note** You can enable or disable TKIP encryption only using the CLI. Configuring TKIP encryption is not supported in GUI. When you have VLAN configuration on WGB, you need to configure the encryption cipher mode and keys for a particular VLAN, for example, **encryption vlan 80 mode ciphers tkip**. Then, you need to configure the encryption cipher mode globally on the multicast interface by entering the following command: **encryption mode ciphers tkip**.
Step 6	**security wpa akm** {**cckm**| **dot1x** | **dot1x-sha256** | **ft** | **psk** |**psk-sha256**} **Example:** `Device(config-wlan)# security wpa akm psk-sha256`	Enable or disable Cisco Centralized Key Management, 802.1x, 802.1x with SHA256 key derivation type, Fast Transition, PSK or PSK with SHA256 key derivation type.

	Command or Action	Purpose
		Note • You cannot enable 802.1x and PSK with SHA256 key derivation type simultaneously. • When you configure Cisco Centralized Key Management SSID, you must enable the **ccx aironet-iesupport** for Cisco Centralized Key Management to work. • WPA3 Enterprise dot1x-sha256 is supported only in local mode.
Step 7	**security wpa psk set-key** {**ascii** | **hex**} {**0** | **8**} *password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 test`	Enter this command to specify a preshared key, if you have enabled PSK. WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
Step 8	**security wpa akm ft** {**dot1x** | **psk**| **sae**} **Example:** `Device(config-wlan)# security wpa akm ft psk`	Enable or disable authentication key management suite for fast transition. **Note** You can now choose between PSK and fast transition PSK as the AKM suite.
Step 9	**security wpa wpa2** **Example:** `Device(config-wlan)# security wpa wpa2`	Enables WPA2.
Step 10	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2` **Example:**	Configure WPA2 cipher. • **aes**—Specifies WPA/AES support.
Step 11	**show wireless pmk-cache**	Displays the remaining time before the PMK cache lifetime timer expires. If you have enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with Cisco Centralized Key Management authenticated key management, the PMK cache lifetime timer is used to trigger reauthentication with the client when necessary. The timer is based on the timeout

	Command or Action	Purpose
		value received from the AAA server or the WLAN session timeout setting. If you configure 802.1x with session timeout between 0 and 299, Pairwise Master Key (PMK) cache is created with a timer of 1 day 84600 seconds. **Note** • The command will show VLAN ID with VLAN pooling feature in VLAN-Override field. • Sticky key caching (SKC) is not supported.

CHAPTER 168

Remote LANs

- Information About Remote LANs, on page 1885
- Configuring Remote LANs (RLANs), on page 1887
- Information About RLAN Authentication Fallback, on page 1900
- Configuring RLAN Authentication Fallback (CLI), on page 1900
- Modifying 802.1X EAP Timers for RLAN Clients, on page 1901
- Verifying RLAN Authentication Fallback, on page 1902

Information About Remote LANs

A Remote LAN (RLAN) is used for authenticating wired clients using the controller. Once the wired client successfully joins the controller, the LAN ports switch the traffic between central or local switching modes. The traffic from wired client is treated as wireless client traffic.

The RLAN in Access Point (AP) sends the authentication request to authenticate the wired client. The authentication of wired client in RLAN is similar to the central authenticated wireless client.

The supported AP models are:

- Cisco Catalyst 9124 Series Access Points
- Cisco Catalyst 9105AXW
- Cisco Aironet OEAP 1810 series
- Cisco Aironet 1815T series
- Cisco Aironet 1810W series
- Cisco Aironet 1815W
- Cisco Catalyst IW6300 Heavy Duty Series Access Points
- Cisco 6300 Series Embedded Services Access Points

Information About Ethernet (AUX) Port

The second Ethernet port in Cisco Aironet 1850, 2800, and 3800 Series APs is used as a link aggregation (LAG) port, by default. It is possible to use this LAG port as an RLAN port when LAG is disabled.

The following APs use LAG port as an RLAN port:

- 1852E
- 1852I
- 2802E
- 2802I
- 3802E
- 3802I
- 3802P
- 4802

Limitation for RLAN

- RLAN supports only a maximum of four wired clients regardless of the AP model.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.

Limitations for Using AUX port in Cisco 2700 Access Points

- RLAN supports AUX port and non-native VLAN for this port.
- Local mode supports wired client traffic on central switch. Whereas, FlexConnect mode does not support central switch.
- FlexConnect mode supports wired client traffic on local switch and not on central switch.
- AUX port cannot be used as a trunk port. Even switches or bridges cannot be added behind the port.
- AUX port does not support dot1x.

Role of Controller

- The controller acts as an authenticator, and Extensible Authentication Protocol (EAP) over LAN (EAPOL) messages from the wired client reaching the controller through an AP.
- The controller communicates with the configured Authentication, Authorization, and Accounting (AAA) server.
- The controller configures the LAN ports for an AP and pushes them to the corresponding AP.

Note

- The RLAN feature is supported on Fabric.
- RLAN is supported in APs that have more than one Ethernet port.
- In RLAN (local mode - local switching mode), if you want to use the AP native VLAN for client IP, the VLAN should be configured as either **no vlan** or **vlan 1** in the RLAN policy profile. For example, if the native VLAN ID is 80, do not use the number 80 in the RLAN policy profile. Also, do not use VLAN name *VLANxxxx* to configure VLAN in the RLAN policy profile.

  When a new client is connected to an AP, the client's details are available in the controller initially. However, after the CAPWAP DOWN/UP state, the client details are no longer listed in the controller.
- APs in local mode central switching do not support VLAN tagged traffic from RLAN clients, and the traffic gets dropped.
- The VLAN name (without any numerals) configured in remote-lan-policy does not provide the mapped VLAN ID for central switching.

Configuring Remote LANs (RLANs)

Enabling or Disabling all RLANs

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **ap remote-lan shutdown** **Example:** `Device(config)# [no] ap remote-lan shutdown`	Enables or disables all RLANs.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating RLAN Profile (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Remote LAN**.

Step 2 Click **Add**.

Step 3 Enter the **Profile Name**, **RLAN ID** and enable or disable the **Status** toggle button. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Click **Apply to Device**.

Creating RLAN Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan profile-name** *remote-lan-profile-name rlan-id* **Example:** `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	Configures remote LAN profile. • *remote-lan-profile*—Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters. • *rlan-id*—Is the remote LAN identifier. Range is from 1 to 128. **Note** You can create a maximum of 128 RLANs. You cannot use the *rlan-id* of an existing RLAN while creating another RLAN. Both RLAN and WLAN profile cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names.

Configuring RLAN Profile Parameters (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Remote LAN**.

Step 2 On the **RLAN Profile** tab, click **Add**.

The **Add RLAN Profile** window is displayed.

Step 3 In the **General** tab:

a) Enter a **Name** and **RLAN ID** for the RLAN profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

b) Set the number of client connections per RLAN in the **Client Association Limit** field.

The range depends on the maximum number of clients supported by the platform.

c) To enable the profile, set the status as **Enable**.

Step 4 In the **Security** > **Layer2** tab

a) To enable 802.1x for an RLAN, set the **802.1x** status as **Enabled**.

Note You can activate either web or 802.1x authentication list at a time.

b) Choose the authorization list name from the **MAC Filtering** drop-down list.

c) Choose the 802.1x for an RLAN authentication list name from the **Authentication List** drop-down list.

Step 5 In the **Security** > **Layer3** tab

a) To enable web authentication for an RLAN, set the **Web Auth** status as **Enabled**.

Note You can activate either web or 802.1x authentication list at a time.

b) Choose the web authentication parameter map from the **Webauth Parameter Map** drop-down list.

c) Choose the web authentication list name from the **Authentication List** drop-down list.

Step 6 In the **Security** > **AAA** tab

a) Set the **Local EAP Authentication** to enabled. Also, choose the required **EAP Profile Name** from the drop-down list.

Step 7 Save the configuration.

Configuring RLAN Profile Parameters (CLI)

Before you begin

The configurations in this section are not mandatory for an RLAN profile.

In case of central switching mode, you need to configure both central switching and central DHCP.

Note The fabric profile configuration is required only for fabric RLAN support.

Procedure

	Command or Action	Purpose
Step 1	**client association limit** *client-connections* **Example:** `Device(config-remote-lan)# client association limit 1`	Configures client connections per RLAN. *client-connections*—Is the maximum client connections per RLAN. Range is from 0 to 10000. 0 refers to unlimited.
Step 2	**fabric-profile** *fabric-profile-name* **Example:** `Device(config-remote-lan)# fabric-profile sample-fabric-profile-name`	Configures fabric profile for RLAN.
Step 3	**ip access-group web** *IPv4-acl-name* **Example:** `Device(config-remote-lan)# ip access-group web acl_name`	Configures RLAN IP configuration commands. *IPv4-acl-name*—Refers to the IPv4 ACL name or ID.
Step 4	**local-auth** *profile name* **Example:** `Device(config-remote-lan)# local-auth profile_name`	Sets EAP Profile on an RLAN. *profile name*—Is the EAP profile on an RLAN.
Step 5	**mac-filtering** *mac-filter-name* **Example:** `Device(config-remote-lan)# mac-filtering mac_filter`	Sets MAC filtering support on an RLAN. *mac-filter-name*—Is the authorization list name.
Step 6	**security dot1x authentication-list** *list-name* **Example:** `Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list`	Configures 802.1X for an RLAN. *list-name*—Is the authentication list name.
Step 7	**security web-auth authentication-list** *list-name* **Example:** `Device(config-remote-lan)# security web-auth authentication-list web_auth_list`	Configures web authentication for an RLAN. *list-name*—Is the authentication list name. **Note** You can activate either web or dot1x authentication list at a time.
Step 8	[**no**] **shutdown** **Example:** `Device(config-remote-lan)# shutdown`	Enables or disables RLAN profile.
Step 9	**end** **Example:** `Device(config-remote-lan)# end`	Returns to privileged EXEC mode.

Creating RLAN Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Remote LAN** > **RLAN Policy**

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Policy Name**.

Step 4 Click **Apply to Device**.

Creating RLAN Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan-policy policy-name** *profile name* **Example:** `Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name`	Configures RLAN policy profile and enters wireless policy configuration mode.

Configuring RLAN Policy Profile Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Remote LAN**.

Step 2 On the **Remote LAN** page, click **RLAN Policy** tab.

Step 3 On the **RLAN Policy** page, click the name of the **Policy** or click **Add** to create a new one.

The **Add/Edit RLAN Policy** window is displayed.

Step 4 In the **General** tab:

a) Enter a **Name** and **Description** for the policy profile.
b) Set **Central Authentication** to **Enabled** state.
c) Set **Central DHCP** to **Enabled** state.
d) Set the **PoE** check box to enable or disable state.
e) To enable the policy, set the status as **Enable**.

Step 5 In the **Access Policies** Tab, choose the VLAN name or number from the **VLAN** drop-down list.

Note When central switching is disabled, the VLAN in the RLAN policy cannot be configured as the AP's native VLAN. To use the AP's native VLAN for client IP, the VLAN should be configured as either **no vlan** or **vlan 1** in the RLAN policy profile.

Step 6 From the **Host Mode** drop-down list, choose the **Host Mode** for the remote-LAN802.1x from the following options:

- Single-Host Mode—Is the default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one.
- Multi-Host Mode—The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed.
- Multi-Domain Mode—The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected.

Note
- For an RLAN profile with open-auth configuration, you must map the RLAN-policy with single host mode. Mapping RLAN-policy with multi-host or multi-domain mode is not supported.
- The controller does not assign data versus voice VLAN, based on traffic. RLAN only supports multiple VLAN assignments through 802.1x AAA override. You must create data and voice VLANs and then assign these VLANs to respective clients, based on their authentication through the 802.1x AAA override.

Step 7 Configure IPv6 ACL or Flexible NetFlow.

- Under the **Access Policies** > **Remote LAN ACL** section, choose the **IPv6 ACL** from the drop-down list.
- Under the **Access Policies** > **AVC** > **Flow Monitor IPv6** section, check the **Egress Status** and **Ingress Status** check boxes and choose the policies from the drop-down lists.

Step 8 Click the **Advanced** tab.

a) Configure the violation mode for Remote-LAN 802.1x from the **Violation Mode** drop-down list, choose the violation mode type from the following options:
   - Shutdown—Disables the port
   - Replace—Removes the current session and initiates authentication for the new host. This is the default behavior.
   - Protect—Drops packets with unexpected MAC addresses without generating a system message.

b) Enter the **Session Timeout (sec)** value to define the client's duration of a session.

   The range is between 20 and 86400 seconds.

c) Under **AAA Policy Params** section, check the **AAA Override** check box to enable AAA override.

d) Under the **Exclusionlist Params** section, check the **Exclusionlist** check box and enter the **Exclusionlist Timeout** value.

   This sets the exclusion time for a client. The range is between 0 and 2147483647 seconds. 0 refers to no timeout.

Step 9 Save the configuration.

Configuring RLAN Policy Profile Parameters (CLI)

Before you begin

RLAN does not support the following features:

- Central Web Authentication (CWA)
- Quality of Service (QoS)
- Bi-Directional Rate Limiting (BDRL)
- Identity PSK (iPSK)

Procedure

	Command or Action	Purpose
Step 1	**central switching** **Example:** `Device(config-remote-lan-policy)# central switching`	Configures central switching.
Step 2	**central dhcp** **Example:** `Device(config-remote-lan-policy)# central dhcp`	Configures central DHCP.
Step 3	**exclusionlist timeout** *timeout* **Example:** `Device(config-remote-lan-policy)# exclusionlist timeout 200`	Sets exclusion-listing on RLAN. *timeout*—Sets the time, up to which the client will be in excluded state. Range is from 0 to 2147483647 seconds. 0 refers to no timeout.
Step 4	**vlan** *vlan* **Example:** `Device(config-remote-lan-policy)# vlan vlan1`	Configures VLAN name or ID. - *vlan*—Is the vlan name.
Step 5	**aaa-override** **Example:** `Device(config-remote-lan-policy)# aaa-override`	Configures AAA policy override.
Step 6	**session-timeout** *timeout in seconds* **Example:** `Device(config-remote-lan-policy)# session-timeout 21`	Configures client session timeout. *timeout in seconds*—Defines the duration of a session. Range is from 20 to 86400 seconds.

	Command or Action	Purpose
		Note If the session timeout is less than 300 seconds for Dot1x clients, the session timeout is set as one day that is, equal to 86400 seconds.
Step 7	**host-mode** {**multidomain** *voice domain* | **multihost** |**singlehost**} **Example:** `Device(config-remote-lan-policy)# host-mode multidomain`	Configures host mode for remote-LAN 802.1x. *voice domain*—Is the RLAN voice domain VLAN ID. Range is from 0 to 65535. You can configure the following IEEE 802.1X authentication modes: • Multi-Domain Mode—The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected. • Multi-Host Mode—The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed. • Single-Host Mode—Is the default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one.
Step 8	**violation-mode** {**protect** | **replace** | **shutdown**} **Example:** `Device(config-remote-lan-policy)# violation-mode protect`	Configures violation mode for Remote-LAN 802.1x. When a security violation occurs, a port is protected based on the following configured violation actions: • Shutdown—Disables the port. • Replace—Removes the current session and initiates authentication for the new host. This is the default behavior. • Protect—Drops packets with unexpected MAC addresses without generating a system message. In the single-host authentication mode, a violation is triggered when more than one device is detected in data VLAN. In a multi-host

	Command or Action	Purpose
		authentication mode, a violation is triggered when more than one device is detected in data VLAN or voice VLAN.
Step 9	[**no**] **poe** **Example:** `Device(config-remote-lan-policy)# poe`	Enables or disables PoE.
Step 10	[**no**] **shutdown** **Example:** `Device(config-remote-lan-policy)# shutdown`	Enables or disables an RLAN policy profile.
Step 11	**end** **Example:** `Device(config-remote-lan-policy)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Policy Tag and Mapping an RLAN Policy Profile to an RLAN Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy remote-lan-policy-tag`	Configures policy tag and enters policy tag configuration mode.
Step 3	**remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id* **Example:** `Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id 2`	Maps an RLAN policy profile to an RLAN profile. • *remote-lan-profile-name*—Is the name of the RLAN profile. • *rlan-policy-profile-name*—Is the name of the policy profile. • *port-id*—Is the LAN port number on the access point. Range is from 1 to 4.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring LAN Port (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap name* **lan port-id** *lan port id* {**disable** | **enable**} **Example:** `Device# ap name L2_1810w_2 lan port-id 1 enable`	Configures a LAN port. • enable—Enables the LAN port. • disable—Disables the LAN port.

Attaching Policy Tag to an Access Point (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Access Points**.

Step 2 Select the AP to attach the Policy Tag.

Step 3 Under the **Tags** section, use the **Policy** drop-down to select a policy tag.

Step 4 Click **Update & Apply to Device**.

Attaching Policy Tag to an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *ap-ethernet-mac* **Example:** `Device(config)# ap 00a2.891c.21e0`	Configures MAP address for an AP and enters AP configuration mode.
Step 3	**policy-tag** *policy-tag-name*	Attaches policy tag to the access point.

	Command or Action	Purpose
	Example: `Device(config-ap-tag)# policy-tag remote-lan-policy-tag`	*policy-tag-name*—Is the name of the policy tag defined earlier.
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying RLAN Configuration

To view the summary of all RLANs, use the following command:

```
Device# show remote-lan summary

Number of RLANs: 1

RLAN        Profile Name                      Status
------------------------------------------------------------------
1            rlan_test_1                       Enabled
```

To view the RLAN configuration by ID, use the following command:

```
Device# show remote-lan id <id>

Remote-LAN Profile Name              : rlan_test_1
================================================
Identifier                                : 1
Status                                    : Enabled
Mac-filtering                             : Not Configured
Number of Active Clients                  : 1
Security_8021X                            : Disabled
8021.x Authentication list name           : Not Configured
Local Auth eap Profile Name               : Not Configured
Web Auth Security                         : Disabled
Webauth Authentication list name          : Not Configured
Web Auth Parameter Map                    : Not Configured
Client association limit                  : 0
Ipv4 Web Pre Auth Acl                     : Not Configured
Ipv6 Web Pre Auth Acl                     : Not Configured
```

To view the RLAN configuration by profile name, use the following command:

```
Device# show remote-lan name <profile-name>

Remote-LAN Profile Name     : rlan_test_1
================================================
Identifier                                  : 1
Status                                      : Enabled
Mac-filtering                               : mac-auth
Number of Active Clients                    : 0
Security_8021x_dot1x                        : Enabled
8021.x Authentication list name             : Not Configured
Local Auth eap Profile Name                 : Not Configured
Web Auth Security                           : Disabled
Webauth Authentication list name            : Not Configured
Web Auth Parameter Map                      : Not Configured
Client association limit                    : 0
Ipv4 Web Pre Auth Acl                       : Not Configured
Ipv6 Web Pre Auth Acl                       : Not Configured
```

```
mDNS Gateway Status                          : Bridge
Fabric Profile Name                        : rlan-fabric-profile
```

To view the detailed output of all RLANs, use the following command:

```
Device# show remote-lan all

Remote-LAN Profile Name            : rlan_test_1
================================================
Identifier                         : 1
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured

Remote-LAN Profile Name            : rlan_test_2
================================================
Identifier                         : 2
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured
```

```
Device# show remote-lan policy summary
Number of Policy Profiles: 1

Profile Name                      Description                              Status
-------------------------------------------------------------------------------------------
rlan_named_pp1                Testing RLAN policy profile              Enabled
```

To view the LAN port configuration of a Cisco AP, use the following command:

```
Device# show ap name <ap_name> lan port summary
LAN Port status for AP L2_1815w_1
Port ID      status       vlanId      poe
-----------------------------------------
LAN1         Enabled       20          Disabled
LAN2         Enabled       20          NA
LAN3         Disabled      0           NA
```

To view the summary of all clients, use the following command:

```
Device# show wireless client summary
Number of Local Clients: 1

MAC Address       AP Name         WLAN         State    Protocol    Method     Role
-------------------------------------------------------------------------------------
d8eb.97b6.fcc6    L2_1815w_1      1            * Run     Ethernet    None       Local
```

To view the client details with the specified username, use the following command:

```
Device# show wireless client username cisco
MAC Address        AP Name          Status      WLAN      Auth Protocol
-------------------------------------------------------------------------------------------------
0014.d1da.a977    L2_1815w_1        Run 1 *      Yes        Ethernet
d8eb.97b6.fcc6    L2_1815w_1        Run 1 *      Yes        Ethernet
```

To view the detailed information for a client by MAC address, use the following command:

```
Device# show wireless client mac-address 2cea.7f18.5bb3 detail
Client MAC Address : 2cea.7f18.5bb3
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.56.33.21
Client IPv6 Addresses : fe80::d60:2e8:4cc2:6212
Client Username: N/A
AP MAC Address : 4ca6.4d22.1a80
AP Name: AP3C57.31C5.799C
AP slot : 16
Client State : Associated
Policy Profile : fabric-rlan-policy
Flex Profile : default-flex-profile
Remote LAN Id: 1 <----------
Remote LAN Name: fabric-rlan <--------
Wireless LAN Network Name (SSID): fabric-rlan <----------
BSSID : 4ca6.4d22.1a81
Connected For : 211 seconds
Protocol : Ethernet <--------
Channel : 0
Port ID: 1 <-----------
Client IIF-ID : 0xa0000002
Association Id : 0
Authentication Algorithm : Open System
<--------o/p trimmed ------>
```

To view the summary of all AP tags, use the following command:

```
Device# show ap tag summary
Number of APs: 2

AP Name             AP Mac               Site Tag Name         Policy Tag Name         RF
Tag Name               Misconfigured     Tag Source
-------------------------------------------------------------------------------------------
L2_1810d_1        0008.3296.24c0       default-site-tag        default-policy-tag
default-rf-tag             No              Default
L2_1810w_2        00b0.e18c.5880       rlan-site-tag              rlan_pt_1
default-rf-tag             No              Static
```

To view the summary of all policy tags, use the following command:

```
Device# show wireless tag policy summary
Number of Policy Tags: 2

Policy Tag Name                   Description
------------------------------------------------------------------------
rlan_pt_1
default-policy-tag                default policy-tag
```

To view details of a specific policy tag, use the following command:

```
Device# show wireless tag policy detailed <rlan_policy_tag_name>
Policy Tag Name : rlan_pt_1
Description     :

Number of WLAN-POLICY maps: 0

Number of RLAN-POLICY maps: 2
```

```
REMOTE-LAN Profile Name           Policy Name                              Port Id

-------------------------------------------------------------------------------------
rlan_test_1                       rlan_named_pp1                             1

rlan_test_1                       rlan_named_pp1                             2
```

To view the fabric client summary, use the following command:

```
Device# show wireless fabric client summary

Number of Fabric Clients : 0

MAC Address    AP Name                          WLAN State              Protocol Method
  L2 VNID    RLOC IP
```

To view the RLAN client summary, use the following command:

```
Device# show wireless client summary

Number of Clients: 1

MAC Address        AP Name       Type  ID  State    Protocol   Method   Role
-------------------------------------------------------------------------------------
2cea.7f18.5bb3 AP3C57.31C5.799C  RLAN   1    Run    Ethernet   None    Local

Number of Excluded Clients: 0
```

Information About RLAN Authentication Fallback

From Cisco IOS XE Cupertino 17.8.1, Remote LAN (RLAN) ports on OfficeExtend Access Points (OEAPs) support the fallback mechanism for authentication from 802.1X to MAC authentication bypass (MAB) and vice versa. If a client using 802.1X as an authentication method fails to authenticate within the timeout period, the client gets authenticated using the MAB method. Similarly, if the device MAC address is not registered for MAB authentication, the authentication fails, and the client gets authenticated using the 802.1X method.

By default, the RLAN fallback mechanism is disabled. You should explicitly enable it. When both 802.1X and MAB are enabled, the device should pass both authentication methods for successful authentication.

Configuring RLAN Authentication Fallback (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan profile-name** *rlan-profile-name rlan-id* **Example:** `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	Configures remote LAN profile.

	Command or Action	Purpose
Step 3	**security** {**dot1x on-macfilter-failure** | **mac-filter on-dot1x-failure**} **Example:** `Device(config-remote-lan)# security dot1x on-macfilter-failure`	Enables 802.1X authentication on MAC filter failure. **Note** You can either configure 802.1X authentication on MAC filter failure or MAC filter authentication on 802.1X failure. You cannot configure both.
Step 4	**end** **Example:** `Device(config-remote-lan)# end`	Returns to privileged EXEC mode.

Modifying 802.1X EAP Timers for RLAN Clients

To adapt the 802.1X EAP timers for RLAN clients, use the following procedure.

Note When you modify the 802.1X EAP timers, ensure that the timer is long enough to allow 802.1X-capable endpoints to authenticate. A timer that is too short may result in 802.1X-capable endpoints being subject to a fallback authentication or authorization technique.

If 802.1X EAP timers are not configured using this procedure, the timer configuration done using the **wireless security dot1x request** and **wireless security dot1x identity-request** commands are applied.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan profile-name** *rlan-profile-name rlan-id* **Example:** `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	Configures the remote LAN profile.
Step 3	**security dot1x identity-request retries** *retry-num* **Example:** `Device(config-remote-lan)# security dot1x identity-request retries 20`	Configures the maximum number of EAP ID request retransmissions. Valid values range from 1 to 20.

	Command or Action	Purpose
Step 4	**security dot1x identity-request timeout** *timeout-value* **Example:** `Device(config-remote-lan)# security dot1x identity-request timeout 120`	Configures the EAP ID request-timeout value, in seconds. Valid values range from 1 to 120.
Step 5	**security dot1x request retries** *retry-num* **Example:** `Device(config-remote-lan)# security dot1x request retries 20`	Configures the maximum number of EAP request retransmissions. Valid values range from 0 to 20.
Step 6	**security dot1x request timeout** *timeout-value* **Example:** `Device(config-remote-lan)# security dot1x request timeout 120`	Configures the EAP request retransmission timeout value, in seconds. Valid values range from 1 to 120.
Step 7	**end** **Example:** `Device(config-remote-lan)# end`	Returns to privileged EXEC mode.

Verifying RLAN Authentication Fallback

To check the status of the fallback authentication mechanism, use the following command:

```
Device# show remote-lan all

Remote-LAN Profile Name     : rlan_profile_name
================================================
Identifier                                    : 3
Status                                        : Disabled
Mac-filtering                                 : Not Configured
Number of Active Clients                      : 0
Security_8021x_dot1x                          : Enabled
8021.x Authentication list name               : Not Configured
Local Auth eap Profile Name                   : Not Configured
Web Auth Security                             : Disabled
Webauth Authentication list name              : Not Configured
Web Auth Parameter Map                        : Not Configured
Client association limit                      : 0
Ipv4 Web Pre Auth Acl                         : Not Configured
Ipv6 Web Pre Auth Acl                         : Not Configured
mDNS Gateway Status                           : Bridge
Authentication Fallback Status                : MAC-filtering to Dot1X
```

CHAPTER 169

RLAN External Module

- Information About External Module, on page 1903
- Prerequisites for Configuring External Module, on page 1903
- Configuring External Module (GUI), on page 1903
- Configuring External Module (CLI), on page 1904
- Verifying External Module, on page 1904

Information About External Module

The External Module feature enables traffic to flow in and out from the Cisco Aironet Developer Platform module when an access point (AP) is in both local and flex connect mode.

Prerequisites for Configuring External Module

Before you begin, you must ensure the following:

- The external module is powered on.
- The RLAN status is enabled.

Configuring External Module (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 In the **Policy** tab, select one of the **Policy Tag Name** and click **Add**.

Step 3 In **Add Policy Tag** page and **RLAN-POLICY Maps** section, click **Add**.

Step 4 From the **Port ID** drop-down list, choose **ext-module**.

Step 5 From the **RLAN Profile** drop-down list, choose an RLAN profile.

Step 6 From the **RLAN Policy Profile** drop-down list, choose an RLAN policy profile.

Step 7 Click the check mark icon.

Configuring External Module (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy default-policy-tag** **Example:** `Device(config)# wireless tag policy default-policy-tag`	Configures a policy tag to the external module for the remote LAN.
Step 3	**remote-lan** *rlan-profile* **policy** *rlan-policy* **ext-module** **Example:** `Device(default-policy-tag)# remote-lan rlan policy abc ext-module`	Configures a remote LAN policy to the external module.

Verifying External Module

To view the external module remote LAN configuration, use the following command:

```
Device# show ap name ap_name lan port summary

LAN Port status for AP ap_name

Port ID      status      vlanId      poe        power-level     RLAN
-------------------------------------------------------------------------
ext-module   Enabled     39          NA         NA              Enabled
```

To view the external module inventory details, use the following command:

```
Device# show ap name abc inventory
NAME: AP3800, DESCR: Cisco Aironet 3800 Series (IEEE 802.11ac) Access Point
PID: AIR-AP3802I-D-K9, VID: 01, SN: xxxxxxxxxxx

MODULE NAME: Expansion Module, DESCR: Cisco HDK Module (rev2)
PID: Unknown, SN: xxxxxxxxxxx, MaxPower: 2700mW
VersionID: V22, Capabilities: RLAN (UP)
```

CHAPTER 170

802.11ax Per WLAN

- Information About 802.11ax Mode Per WLAN, on page 1905
- Configuring 802.11ax Mode Per WLAN (GUI), on page 1905
- Configuring 802.11ax Mode Per WLAN (CLI), on page 1906
- Verifying 802.11ax Mode Per WLAN, on page 1906

Information About 802.11ax Mode Per WLAN

Prior to Cisco IOS XE Bengaluru Release 17.4.1, the 802.11ax mode was configured per radio band. In this configuration, the 11ax mode was either enabled or disabled for all WLANs (AP) that were configured per radio, all at once. When 11ax was enabled per radio, the 11ac clients were not able to scan or connect to the SSID if the beacon had 11ax information elements. Client could not probe an access point (AP), if the beacon has 11ax IE.

Therefore, a 11ax configuration knob per AP is introduced, from Cisco IOS XE Bengaluru Release 17.5.1. This knob is introduced under the WLAN profile. By default, the 11ax knob per WLAN is now enabled on the controller.

Note For 6-GHz radio, the 802.11ax parameters are taken from the multi BSSID profile tagged to the corresponding 6-GHz RF profile of the AP. So, the WLAN dot11ax parameters are overridden by multi BSSID profile parameters in the case of 6-GHz. There are no changes for 2.4 and 5-GHz band WLANs. They continue to use the WLAN parameters for 802.11ax.

Configuring 802.11ax Mode Per WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.
The **Add WLAN** window is displayed.

Step 3 Click the **Advanced** tab.

Step 4 In the **11ax** section, check the **Enable 11ax** check box to enable 802.11ax operation status on the WLAN.

Note When 11ax is disabled, beacons will not display 11ax IE, and all the 11ax features will be operationally disabled on the WLAN.

Step 5 Click **Apply to Device**.

Configuring 802.11ax Mode Per WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile-name* **Example:** `Device(config)# wlan wlan-profile`	Specifies the WLAN name and enters the WLAN configuration mode.
Step 3	**dot11ax** **Example:** `Device(config-wlan)# dot11ax`	Configures 802.11ax on a WLAN.
Step 4	**no dot11ax** **Example:** `Device(config-wlan)# no dot11ax`	Disables 802.11ax on the WLAN profile.

Verifying 802.11ax Mode Per WLAN

To display the status of the 11ax parameter, run the following command:

```
Device# show wlan id 6
WLAN Profile Name     : power
===============================================
Identifier                                : 6
Description                               :
Network Name (SSID)                       : power
Status                                    : Enabled
Broadcast SSID                            : Enabled
Advertise-Apname                          : Disabled
Universal AP Admin                        : Disabled
Max Associated Clients per WLAN           : 0
Max Associated Clients per AP per WLAN    : 0
Max Associated Clients per AP Radio per WLAN   : 200
.
.
.
```

```
802.11ac MU-MIMO                                : Enabled
802.11ax parameters
    802.11ax Operation Status                   : Enabled
    OFDMA Downlink                              : Enabled
    OFDMA Uplink                                : Enabled
    MU-MIMO Downlink                            : Enabled
    MU-MIMO Uplink                              : Enabled
    BSS Target Wake Up Time                     : Enabled
    BSS Target Wake Up Time Broadcast Support   : Enabled
.
.
.
```

CHAPTER 171

BSS Coloring

- Information About BSS Coloring , on page 1909
- Configuring BSS Color on AP (GUI), on page 1910
- Configuring BSS Color in the Privileged EXEC Mode, on page 1911
- Configuring BSS Color Globally (GUI), on page 1911
- Configuring BSS Color in the Configuration Mode, on page 1912
- Configuring Overlapping BSS Packet Detect (GUI), on page 1912
- Configuring OBSS-PD Spatial Reuse Globally (CLI), on page 1913
- Configuring OBSS PD in an RF Profile (GUI), on page 1913
- Configuring OBSS-PD Spatial Reuse in the RF Profile Mode (CLI), on page 1914
- Verifying BSS Color and OBSS-PD, on page 1914

Information About BSS Coloring

The 802.11 Wi-Fi standard minimizes the chance of multiple devices interfering with one another by transmitting at the same time. This carrier-sense multiple access with collision avoidance (CSMA/CA) technology is based on static thresholds that allow Wi-Fi devices to avoid interfering with each other on air. However, with an increase in density and the number of Wi-Fi devices, these static thresholds often lead to CSMA/CA causing devices to defer transmissions unnecessarily.

For example, if two devices that are associated with different BSS, can hear every transmission from each other at relatively low signal strengths, each device should defer its transmission when it receives a transmission from the other. But if both the devices were to transmit at the same time, it is likely that neither would cause enough interference at the other BSS' receiver to cause reception failure for either transmission.

Devices today must demodulate packets to look at the MAC header in order to determine whether or not a received packet belongs to their own BSS. This process of demodulation consumes power, which can be saved if devices can quickly identify the BSS by looking at the PHY header alone, and subsequently drop packets that are from a different BSS. Prior to Wi-Fi 6, there was no provision for devices to do this.

The new 802.11ax (Wi-Fi 6) standard addresses both of the issues discussed above, through the new BSS Coloring and Spatial Reuse mechanism. BSS Coloring is a new provision that allows devices operating in the same frequency space to quickly distinguish between packets from their own BSS and packets from an Overlapping BSS (OBSS), by simply looking at the BSS color value contained in the HE PHY header. In some scenarios, Spatial Reuse allows devices, to transmit at the same time as the OBSS packets they receive, instead of deferring transmissions because of legacy interference thresholds. Since every Wi-Fi 6 device understands the BSS color, it can be leveraged to increase power savings by dropping packets earlier, and to identify spatial reuse opportunities.

BSS Coloring

BSS Coloring is a method used to differentiate between the BSS of access points and their clients on the same RF channel. Wi-Fi 6 enables each AP radio to assign a value (from 1 to 63), known as BSS color, to be included in the PHY header of all HE transmissions from devices in its BSS. With devices of each BSS transmitting a locally-unique color, a device can quickly and easily distinguish transmissions coming from its BSS from those of a neighboring BSS.

The following platforms support this feature:

- Cisco Catalyst 9800 Series Wireless Controllers
- Cisco Catalyst 9115 Access Points
- Cisco Catalyst 9120AX Series Access Points
- Cisco Catalyst 9124AX Series Access Points
- Cisco Catalyst 9130AX Access Points

OBSS-PD and Spatial Reuse

Overlapping BSS Packet Detect (OBSS-PD) is a more aggressive Wi-Fi packet detect threshold for inter-BSS packets, which can be higher than the typical/legacy -82 dBm. Inter-BSS packets are easily identified by comparing the BSS color in the HE PHY header of the packets received with the BSS color of the device.

In OBSS-PD based Spatial Reuse, to improve throughput and network efficiency by increasing transmitting opportunities, a Wi-Fi 6 or 802.11ax device can transmit over an inter-BSS packet with an RSSI that is below the OBSS-PD threshold instead of deferring.

Note Cisco Catalyst 9120AX Series Access Points do not support OBSS-PD.

Configuring BSS Color on AP (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Access Points**.

Step 2 Click the **5 GHz Radios** section or the **2.4 GHz Radios** section.
The list of the AP radios in the band is displayed.

Step 3 Click the required AP name.
The **Edit Radios** window is displayed.

Step 4 From the **Edit Radios** window, select the **Configure** tab.
The general information, Antenna Parameters, RF Channel Assignment, Tx Power Level Assignment, and BSS Color are displayed.

Step 5 In the **BSS Color** area and from the **BSS Color Configuration** drop-down list, choose **Custom** configuration

- **Custom**: To manually select the BSS color configuration for the AP radio.

a. Click the **BSS Color Status** field to disable or enable the feature.

b. In the **Current BSS Color** field, specify a corresponding BSS color for the AP radio. The valid range is between 1 and 63.

Step 6 Click **Update & Apply to Device**.

Configuring BSS Color in the Privileged EXEC Mode

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

Step 2	**ap name** *ap-name* **dot11** { **24ghz** | **5ghz** | **6ghz** | **dual-band** [**slot** *slot-id*] } **dot11ax bss-color** *<1-63>*
	Example:
	`Device#ap name apn dot11 24ghz slot 0 dot11ax bss-color 12`
	Example:
	`Device#ap name apn no dot11 24ghz slot 0 dot11ax bss-color`
		Sets the BSS color on the 2.4-GHz, 5-GHz, 6-GHz, or dual-band radio, for a specific access point on the following slots:
		• 5 GHz: Slot 1 and 2
		• 2.4 GHz: Slot 0
		• 6-GHz: Slot 3
		• Dual-band: Slot 0
		Use the `no` form of this command to disable BSS color.

Configuring BSS Color Globally (GUI)

Procedure

Step 1 Choose **Configuration > Radio Configurations > Parameters**.

Step 2 In the **11ax Parameters** section, enable BSS color globally for the 5 GHz and 2.4 GHz radios by checking the **BSS Color** check box.

Configuring BSS Color in the Configuration Mode

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**[no] ap dot11** { **24ghz** | **5ghz** | **6ghz** } **dot11ax bss-color** **Example:** `Device(config)#[no] ap dot11 24ghz dot11ax bss-color`	Enables the 802.11ax BSS color on all 2.4-GHz or 5-GHz or 6-GHz radios. Use the `no` form of this command to disable BSS color.

Configuring Overlapping BSS Packet Detect (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **Parameters**.

The parameters page is displayed where you can configure global parameters for 5 GHz Band and 2.4 GHz Band radios.

Step 2 In the **11ax Parameters** section, check the **OBSS PD** check box to enable the overlapping BSS packet detect (OBSS PD) feature.

Step 3 In the **Non-SRG OBSS PD Max Threshold** field, enter the threshold in decibel-milliwatts. Value range is between -82 dBm and -62 dBm.

Configuring OBSS-PD Spatial Reuse Globally (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**[no] ap dot11** {**24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd** **Example:** `Device(config)#[no] ap dot11 24ghz dot11ax spatial-reuse obss-pd`	Configures 802.11ax OBSS PD based spatial reuse on all 2.4-GHz or 5-GHz radios. Use the `no` form of this command to disable this feature.
Step 3	**ap dot11** {**24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62* **Example:** `Device(config)#[no] ap dot11 24ghz dot11ax spatial-reuse obss-pd non-srg-max -62`	Configure 802.11ax non-SRG OBSS PD max on all 2.4-GHz or 5-GHz radios. The default value is -62.

Configuring OBSS PD in an RF Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF**.

Step 2 On the **RF Profile** page, click **Add** to configure the following:

- General
- 802.11
- RRM
- Advanced

Step 3 In the **Advanced** tab, under the **11ax Parameters** section, complete the following:

a) Use the toggle button to enable or disable the **OBSS PD** field.

b) In the **Non-SRG OBSS PD Max Threshold (dBm)**, enter the threshold value. The default value is -62 dBm. Values range between -82 dBm and -62 dBm.

Step 4 Click **Save & Apply to Device**.

Configuring OBSS-PD Spatial Reuse in the RF Profile Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** { **24ghz | 5ghz | 6ghz** } **rf-profile** *rf-profile-name* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**[no] dot11ax spatial-reuse obss-pd** **Example:** `Device(config-rf-profile)#[no] dot11ax spatial-reuse obss-pd`	Configures 802.11ax OBSS PD based spatial reuse in the RF profile configuration mode. Use the `no` form of this command to disable this feature.
Step 4	**dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62* **Example:** `Device(config-rf-profile)# dot11ax spatial-reuse obss-pd non-srg-max -62`	Configure 802.11ax non-SRG OBSS PD max on all 2.4-GHz or 5-GHz or 6-GHz radios. The default value is -62.

Verifying BSS Color and OBSS-PD

To verify if the global per-band BSS color and OBSS-PD are enabled, use the following **show** command:

```
Device# show ap dot11 24ghz network
802.11b Network                          : Enabled
11gSupport                               : Enabled
11nSupport                               : Enabled
.
.
.
802.11ax                                 : Enabled
  DynamicFrag                            : Enabled
  MultiBssid                             : Enabled
  Target Wakeup Time                     : Enabled
  Target Wakeup Time Broadcast           : Enabled
  BSS Color                              : Enabled
  OBSS PD                                : Enabled
  Non-SRG OBSS PD Max                    : -62 dBm
802.11ax MCS Settings:
  MCS  7, Spatial Streams = 1            : Supported
.
.
.
```

To view the RF profile OBSS-PD configuration, use the following **show** command:

```
Device# show ap rf-profile name rf-profile-name detail
Description                     : pre configured rfprofile for 5gh radio
RF Profile Name                 : rf-profile-name
Band                            : 5 GHz
Transmit Power Threshold v1     : -65 dBm
Min Transmit Power              : 7 dBm
Max Transmit Power              : 30 dBm
.
.
.
802.11ax
  OBSS PD                       : Enabled
  Non-SRG OBSS PD Max           : -62 dBm
NDP mode                        : Auto
```

To view the BSS color configuration of all the AP radios on a band in the summary list, along with Channel, TX Power and so on, use the following **show** command:

```
Device# show ap dot11 24ghz summary extended
AP Name                         Mac Address     Slot    Admin State    Oper State    Width
  Txpwr           Channel                       BSS Color
------------------------------------------------------------------------------------------

Ed2-JFW-AP1                     84b2.61ba.4730  1       Enabled        Up            40
    1/6 (17 dBm)    (136,132)*
11AX-9120-AP1                   d4ad.bda2.3fc0  1       Enabled        Up            20
    1/8 (23 dBm)    (36)                         30
Ed2-JFW-AP2                     f8c2.8885.59f0  1       Enabled        Up            20
    1/5 (15 dBm)    (40)
```

To view the BSS color configuration and the capability of an AP radio, use the following **show** commands:

```
Device# show ap name AP7069.5A74.816C config dot11 24ghz
Cisco AP Identifier                             : 502f.a876.1e60
Cisco AP Name                                   : AP7069.5A74.816C
Attributes for Slot 0
  Radio Type                                    : 802.11b
  Radio Mode                                    : REAP
  Radio Role                                    : Auto
  Radio SubType                                 : Main
  Administrative State                          : Enabled
  Operation State                               : Up
  .
  .
  .
Phy OFDM Parameters
    Configuration                               : Automatic
    Current Channel                             : 6
    Channel Width                               : 20 MHz
    TI Threshold                                : 1157693440
    Antenna Type                                : External
    External Antenna Gain (in .5 dBi units)     : 8
    .
    .
    .
  !BSS color details are displayed below:
  802.11ax Parameters
    HE Capable                                  : Yes
    BSS Color Capable                           : Yes
    BSS Color Configuration                     : Customized
    Current BSS Color                           : 34

Device# show ap name AP70XX.5XX4.8XXX config slot 0
Cisco AP Identifier                             : 502f.a876.1e60
```

```
Cisco AP Name                                   : AP70XX.5XX4.8XXX
Country Code                                    : US
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -A
MAC Address                                     : 7069.5a74.816c
IP Address Configuration                        : DHCP
IP Address                                      : Disabled
.
.
.
Attributes for Slot 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Radio Role                                    : Auto
  Radio Mode                                    : REAP
  Radio SubType                                 : Main
  Administrative State                          : Enabled
.
.
.
  Phy OFDM Parameters
    Configuration                               : Automatic
    Current Channel                             : 6
    Channel Assigned By                         : DCA
    Extension Channel                           : NONE
    Channel Width                               : 20
    Allowed Channel List                        : 1,2,3,4,5,6,7,8,9,10,11
    TI Threshold                                : 1157693440
    DCA Channel List                            :
    Antenna Type                                : EXTERNAL_ANTENNA
    External Antenna Gain (in .5 dBi units)     : 8
Diversity                                       : DIVERSITY_ENABLED
    802.11n Antennas
      A                                         : ENABLED
      B                                         : ENABLED
      C                                         : ENABLED
      D                                         : ENABLED
  .
  .
  .
  !BSS color details are displayed below:
  802.11ax Parameters
    HE Capable                                  : Yes
    BSS Color Capable                           : Yes
    BSS Color Configuration                     : Customized
    Current BSS Color                           : 34
.
.
.
```

CHAPTER 172

DHCP for WLANs

- Information About Dynamic Host Configuration Protocol, on page 1917
- Restrictions for Configuring DHCP for WLANs, on page 1920
- Guidelines for DHCP Relay Configuration, on page 1920
- How to Configure DHCP for WLANs, on page 1921
- Configuring the Internal DHCP Server, on page 1923
- Configuring DHCP-Required for FlexConnect, on page 1933

Information About Dynamic Host Configuration Protocol

You can configure WLANs to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available—internal and external.

Internal DHCP Servers

The device contains an internal DHCP server. This server is typically used in branch offices that do not have a DHCP server.

The internal server provides DHCP addresses to wireless clients, direct-connect APs, and DHCP requests that are relayed from APs. Only lightweight APs are supported. If you want to use the internal DHCP server, ensure that you configure SVI for the client VLAN, and set the IP address as DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the APs must use an alternative method to locate the management interface IP address of the device, such as local subnet broadcast, Domain Name System (DNS), or priming.

When clients use the internal DHCP server of the device, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned to the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one.

Note

- VRF is supported in the internal DHCP servers.
- DHCPv6 is not supported in the internal DHCP servers.

General Guidelines

- Internal DHCP server serves both wireless client and wired client (wired client includes AP).
- To serve wireless client with internal DHCP server, an unicast DHCP server IP address must be configured for wireless client. Internal DHCP server IP address must be configured under the server facing interface, which can be loopback interface, SVI interface, or L3 physical interface.
- To use internal DHCP server for both wireless and wired client VLAN, an IP address must be configured under client VLAN SVI interface.
- For wireless client, in DHCP helper address configuration, the IP address of the internal DHCP server must be different from address of wireless client VLAN SVI interface.
- For wireless client with internal DHCP server support, the internal DHCP server can be configured using global configuration command, under the client VLAN SVI interface or under the wireless policy profile.
- An internal DHCP server pool can also serve clients of other controllers .

External DHCP Servers

The operating system is designed to appear as a DHCP relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay, which means that each controller appears as a DHCP relay agent to the DHCP server, and as a DHCP server in the virtual IP address to wireless clients.

Because the controller captures the client IP address that is obtained from a DHCP server, it maintains the same IP address for that client during intra controller, inter controller, and inter-subnet client roaming.

Note External DHCP servers support DHCPv6.

DHCP Assignments

You can configure DHCP on a per-interface or per-WLAN basis. We recommend that you use the primary DHCP server address that is assigned to a particular interface.

You can assign DHCP servers for individual interfaces. You can configure the management interface, AP manager interface, and dynamic interface for a primary and secondary DHCP server, and configure the service-port interface to enable or disable DHCP servers. You can also define a DHCP server on a WLAN (in this case, the server overrides the DHCP server address on the interface assigned to the WLAN).

Security Considerations

For enhanced security, we recommend that you ask all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all the WLANs with a DHCP Address. Assignment Required setting, which disallows client static IP addresses. If DHCP Address Assignment Required is selected, clients must obtain an IP address through DHCP. Any client with a static IP address is not allowed on the network. The controller monitors DHCP traffic because it acts as a DHCP proxy for the clients.

Note

- WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server.
- The operating system is designed to appear as a DHCP relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP relay. This means that each controller appears as a DHCP relay to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

You can create WLANs with DHCP Address Assignment Required disabled. If you do this, clients have the option of using a static IP address or obtaining an IP address from a designated DHCP server. However, note that this might compromise security.

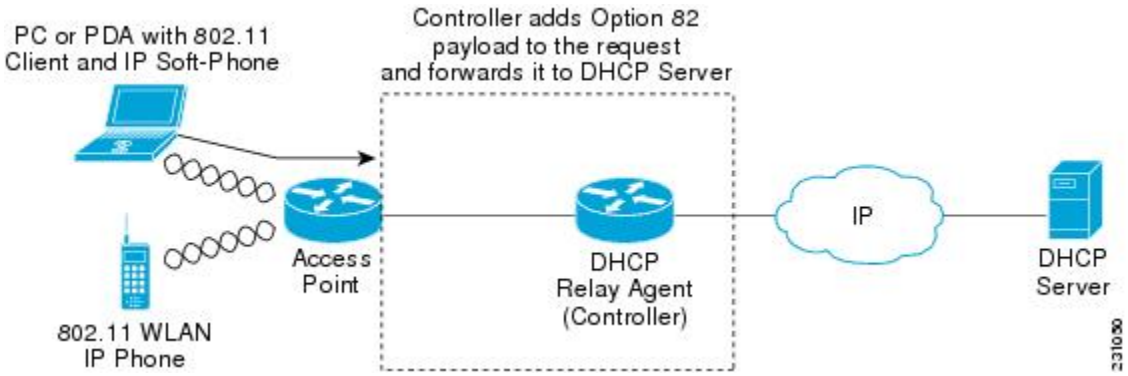
Note DHCP Address Assignment Required is not supported for wired guest LANs.

You can create separate WLANs with DHCP Address Assignment Required configured as disabled. This is applicable only if DHCP proxy is enabled for the controller. You must not define the primary or secondary configuration DHCP server instead you should disable the DHCP proxy. These WLANs drop all the DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

DHCP Option 82

DHCP option 82 provides additional security when DHCP is used to allocate network addresses. It enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can configure the controller to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.

Figure 52: DHCP Option 82



The AP forwards all the DHCP requests from a client to the controller. The controller adds the DHCP option 82 payload and forwards the request to the DHCP server. The payload can contain the MAC address or the MAC address and SSID of the AP, depending on how you configure this option.

Note DHCP packets that already include a relay agent option are dropped at the controller.

For DHCP option 82 to operate correctly, DHCP proxy must be enabled.

Restrictions for Configuring DHCP for WLANs

- If you override the DHCP server in a WLAN, you must ensure that you configure the underlying Cisco IOS configuration to make sure that the DHCP server is reachable.
- WLAN DHCP override works only if DHCP service is enabled on the controller.

  You can configure DHCP service in either of the following ways:

  - Configuring the DHCP pool on the controller.
  - Configuring a DHCP relay agent on the SVI. Note that the VLAN of the SVI must be mapped to the WLAN where DHCP override is configured.

Guidelines for DHCP Relay Configuration

Relay Agent Source IP

- If you configure source interface VLAN in the SVI interface, the IP address of the VLAN interface configured as source is used.
- If the Relay Agent source IP is not mentioned, the IP address of the SVI interface created for the corresponding client's VLAN is used.
- If the Relay Agent source IP is not mentioned, the source address specified at the global level is used.

Note

- The DHCP packets are sourced from the IP address of the Wireless Management Interface (WMI), if VLAN is not configured in the policy profile and AAA override.
- The SVI interface configuration is mandatory to achieve the DHCP relay functionality in central DHCP or local switching.
- Even though many interface options are available in the **ip dhcp relay source-interface** <> command, only VLAN interface is applicable.

DHCP Server

- If the DHCP server address is configured in the wireless policy profile, the server address configured in the policy profile takes precedence.

- If the DHCP server address is not configured in the policy profile, the server address configured in SVI takes precedence.

Note You can configure two server addresses in the SVI. In this case, the DHCP packets from the client are sent to both the servers.

The Option 82 configured in policy profile, SVI, and globally is considered and honored together.

How to Configure DHCP for WLANs

Configuring DHCP Scopes (GUI)

Procedure

Step 1 Choose **Administration** > **DHCP Pools**.

Step 2 In the **Pools** section, click **Add** to add a new DHCP pool.

The **Create DHCP Pool** dialog box is displayed.

Step 3 In the **DHCP Pool Name** field, enter a name for the new DHCP pool.

Step 4 From the **IP Type** drop-down list, choose the IP address type.

Step 5 In the **Network** field, enter the network served by this DHCP scope. This IP address is used by the management interface with netmask applied, as configured in the **Interfaces** window.

Step 6 In the **Subnet Mask** field, enter the subnet mask assigned to all the wireless clients.

Step 7 In the **Starting ip** field, enter the starting IP address.

Step 8 In the **Ending ip** field, enter the trailing IP address.

Step 9 In the **Reserved Only** field, enable or disable it.

Step 10 From the **Lease** drop-down list, choose the lease type as either **User Defined** or **Never Expires**. If you choose User Defined, you can enter the amount of time that an IP address is granted to a client.

Step 11 To perform advanced configuration for DHCP scope, click **Advanced**.

Step 12 Check the **Enable DNS Proxy** check box to enable DNS proxy.

Step 13 In the **Default Router(s)** field, enter the IP address of the optional router or routers that connect to the device and click the + icon to add them to the list. Each router must include a DHCP forwarding agent that enables a single device to serve the clients of multiple devices.

Step 14 In the **DNS Server(s)** field, enter the IP address of the optional DNS server or servers and click the + icon to add them to the list. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by the DHCP scope.

Step 15 In the **NetBios Name Server(s)** field, enter the IP address of the optional Microsoft NetBIOS name server or servers, such as Microsoft Windows Internet Naming Service (WINS) server, and click the + icon to add them to the list.

Step 16 In the **Domain** field, enter the optional domain name of the DHCP scope for use with one or more DNS servers.

Step 17 To add **DHCP** options, click **Add** in the **DHCP Options List** section. DHCP provides an internal framework for passing configuration parameters and other control information, such as DHCP options, to the clients on your network. DHCP options carry parameters as tagged data stored within protocol messages exchanged between the DHCP server and its clients.

Step 18 Enter the **DHCP** option that you want to add.

Step 19 Click **Save & Apply to Device**.

Configuring DHCP Scopes (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool test-pool`	Configures the DHCP pool address.
Step 3	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 209.165.200.224 255.255.255.0`	Specifies the network number in dotted-decimal notation and the mask address.
Step 4	**dns-server** *hostname* **Example:** `Device(dhcp-config)# dns-server example.com`	Specifies the DNS name server. You can specify an IP address or a hostname.
Step 5	**end** **Example:** `Device(dhcp-config)# end`	Returns to privileged EXEC mode.

Configuring the Internal DHCP Server

Configuring the Internal DHCP Server Under Client VLAN SVI (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** > **SVI**.

Step 2 Click an SVI.

Step 3 Click the **Advanced** tab.

Step 4 Under **DHCP Relay** settings, enter the **IPV4 Helper Address**.

Step 5 Click **Update & Apply to Device**.

Configuring the Internal DHCP Server Under Client VLAN SVI (CLI)

Before you begin

- For wireless clients, only two DHCP servers are supported.
- To use the internal DHCP server for both wireless and wired client VLAN, an IP address must be configured under the client VLAN SVI.
- For wireless clients, the IP address of the internal DHCP server must be different from the address of the wireless client VLAN SVI (in the DHCP helper address configuration).
- For wireless clients, the internal DHCP server can be configured under the client VLAN SVI or under the wireless policy profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface loopback** *interface-number* **Example:** `Device(config)# interface Loopback0`	Creates a loopback interface and enters interface configuration mode.
Step 3	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	Configures the IP address for the interface.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 5	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 32`	Configures the VLAN ID.
Step 6	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 192.168.32.100 255.255.255.0`	Configures the IP address for the interface.
Step 7	**ip helper-address** *ip-address* **Example:** `Device(config-if)# ip helper-address 10.10.10.1`	Configures the destination address for UDP broadcasts. **Note** If the IP address used in the **ip helper-address** command is an internal address of the controller an internal DHCP server is used. Otherwise, the external DHCP server is used.
Step 8	**no mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the Maintenance Operation Protocol (MOP) for an interface.
Step 9	**no mop sysid** **Example:** `Device(config-if)# no mop sysid`	Disables the task of sending MOP periodic system ID messages.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 11	**ip dhcp excluded-address** *ip-address* **Example:** `Device(config)# ip dhcp excluded-address 192.168.32.1`	Specifies the IP address that the DHCP server should not assign to DHCP clients.
Step 12	**ip dhcp excluded-address** *ip-address* **Example:** `Device(config)# ip dhcp excluded-address 192.168.32.100`	Specifies the IP addresses that the DHCP server should not assign to DHCP clients.

	Command or Action	Purpose
Step 13	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool pool-vlan32`	Configures the DHCP pool address.
Step 14	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	Specifies the network number in dotted-decimal notation, along with the mask address.
Step 15	**default-router** *ip-address* **Example:** `Device(dhcp-config)# default-router 192.168.32.1`	Specifies the IP address of the default router for a DHCP client.
Step 16	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP configuration mode.
Step 17	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 18	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 19	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Configures the central DHCP for locally switched clients.
Step 20	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures WLAN for central switching.
Step 21	**description** *policy-proile-name* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile
Step 22	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.

	Command or Action	Purpose
Step 23	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless profile policy.

Configuring the Internal DHCP Server Under a Wireless Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click a policy name.

Step 3 Click the **Advanced** tab.

Step 4 Under **DHCP** settings, check or uncheck the **IPv4 DHCP Required** check box and enter the **DHCP Server IP Address**.

Step 5 Click **Update & Apply to Device**.

Configuring the Internal DHCP Server Under a Wireless Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface loopback** *interface-number* **Example:** `Device(config)# interface Loopback0`	Creates a loopback interface and enters interface configuration mode.
Step 3	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	Configures the IP address for the interface.
Step 4	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 5	**interface vlan** *vlan-id* **Example:**	Configures the VLAN ID.

	Command or Action	Purpose
	`Device(config)# interface vlan 32`	
Step 6	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 192.168.32.100 255.255.255.0`	Configures the IP address for the interface.
Step 7	**no mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the Maintenance Operation Protocol (MOP) for an interface.
Step 8	**no mop sysid** **Example:** `Device(config-if)# no mop sysid`	Disables the task of sending MOP periodic system ID messages.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 10	**ip dhcp excluded-address** *ip-address* **Example:** `Device(config)# ip dhcp excluded-address 192.168.32.100`	Specifies the IP address that the DHCP server should not assign to DHCP clients.
Step 11	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool pool-vlan32`	Configures the DHCP pool address.
Step 12	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	Specifies the network number in dotted-decimal notation along with the mask address.
Step 13	**default-router** *ip-address* **Example:** `Device(dhcp-config)# default-router 192.168.32.1`	Specifies the IP address of the default router for a DHCP client.
Step 14	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP configuration mode.
Step 15	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile and enters wireless policy configuration mode.

	Command or Action	Purpose
Step 16	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 17	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures local switching.
Step 18	**description** *policy-proile-name* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile.
Step 19	**ipv4 dhcp opt82** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82`	Enables DHCP Option 82 for the wireless clients.
Step 20	**ipv4 dhcp opt82 ascii** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	Enables ASCII on DHCP Option 82.
Step 21	**ipv4 dhcp opt82 format vlan_id** **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan32`	Enables VLAN ID.
Step 22	**ipv4 dhcp opt82 rid** *vlan_id* **Example:** `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	Supports the addition of Cisco 2-byte Remote ID (RID) for DHCP Option 82.
Step 23	**ipv4 dhcp server** *ip-address* **Example:** `Device(config-wireless-policy)#  ipv4 dhcp server 10.10.10.1`	Configures the WLAN's IPv4 DHCP server.
Step 24	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.
Step 25	**no shutdown** **Example:**	Enables the wireless profile policy.

	Command or Action	Purpose
	`Device(config-wireless-policy)# no shutdown`	

Configuring the Internal DHCP Server Globally (GUI)

Procedure

Step 1 Choose **Administration** > **DHCP Pools** > **Pools**.

Step 2 Click **Add**.

The **Create DHCP Pool** window is displayed.

Step 3 Enter the **DHCP Pool Name**, **Network**, **Starting ip**, and **Ending ip**.

Step 4 From the **IP Type**, **Subnet Mask**, and **Lease** drop-down lists, choose a value.

Step 5 Click the **Reserved Only** toggle button.

Step 6 Click **Apply to Device**.

Configuring the Internal DHCP Server Globally (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface loopback** *interface-num* **Example:** `Device(config)# interface Loopback0`	Creates a loopback interface and enters interface configuration mode.
Step 3	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	Configures the IP address for the interface.
Step 4	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 5	**interface vlan***vlan-id* **Example:** `Device(config)# interface vlan 32`	Configures the VLAN ID.

	Command or Action	Purpose
Step 6	**ip address** *ip-address* **Example:** `Device(config-if)# ip address 192.168.32.100 255.255.255.0`	Configures the IP address for the interface.
Step 7	**no mop enabled** **Example:** `Device(config-if)# no mop enabled`	Disables the Maintenance Operation Protocol (MOP) for an interface.
Step 8	**no mop sysid** **Example:** `Device(config-if)# no mop sysid`	Disables the task of sending the MOP periodic system ID messages.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits the interface configuration mode.
Step 10	**ip dhcp-server** *ip-address* **Example:** `Device(config)# ip dhcp-server 10.10.10.1`	Specifies the target DHCP server parameters.
Step 11	**ip dhcp excluded-address** *ip-address* **Example:** `Device(config)# ip dhcp excluded-address 192.168.32.100`	Specifies the IP address that the DHCP server should not assign to DHCP clients.
Step 12	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool pool-vlan32`	Configures the DHCP pool address.
Step 13	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	Specifies the network number in dotted-decimal notation along with the mask address.
Step 14	**default-router** *ip-address* **Example:** `Device(dhcp-config)# default-router 192.168.32.1`	Specifies the IP address of the default router for a DHCP client.
Step 15	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP configuration mode.

	Command or Action	Purpose
Step 16	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 17	**central association** **Example:** `Device(config-wireless-policy)# central association`	Configures central association for locally switched clients.
Step 18	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Configures central DHCP for locally switched clients.
Step 19	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures local switching.
Step 20	**description** *policy-proile-name* **Example:** `Device(config-wireless-policy)# description "default policy profile"`	Adds a description for the policy profile.
Step 21	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 32`	Assigns the profile policy to the VLAN.
Step 22	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the profile policy.

Configuring IP Reservations in the Internal DHCP Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool dhcp-pool-add`	Configures the DHCP pool address.
Step 3	**network** *network-name mask-address* **Example:** `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	Specifies the network number in dotted-decimal notation along with the mask address.
Step 4	**address** *ip-address* {**client-id** *client-id* | **hardware-address** *client-mac-id*} **Example:** `Device(dhcp-config)# address 209.165.200.224 client-id dhcp-client-id`	Configures a reserved address using either the client ID or the MAC address. **Note** The IP reservation is contingent on the type of identifier, be it the client ID or the MAC address that the client provides. If the client sends its DHCP DISCOVER or REQUEST using the client ID, set your IP reservation using the client ID and not the hardware address.

Verifying Internal DHCP Configuration

To verify client binding, use the following command:

```
Device# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State
Interface
                Hardware address/
                User name
192.168.32.3    0130.b49e.491a.53       Mar 23 2018 06:42 PM    Automatic  Active
Loopback0
```

To verify the DHCP relay statistics for a wireless client, use the following command:

```
Device# show wireless dhcp relay statistics

DHCP Relay Statistics
---------------------

DHCP Server IP :   10.10.10.1

Message              Count
--------------------------
DHCPDISCOVER      :  1
BOOTP FORWARD     :  137
BOOTP REPLY       :  0
DHCPOFFER         :  0
DHCPREQUEST       :  54
```

```
DHCPACK           :  0
DHCPNAK           :  0
DHCPDECLINE       :  0
DHCPRELEASE       :  0
DHCPINFORM        :  82

Tx/Rx Time :
------------
LastTxTime : 18:42:18
LastRxTime : 00:00:00

Drop Counter :
-------------
TxDropCount : 0
```

To verify the DHCP packet punt statistics in CPP, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless punt statistics

CPP Wireless Punt stats:

                                App Tag     Packet Count
                                -------     ------------
          CAPWAP_PKT_TYPE_DOT11_PROBE_REQ           14442
               CAPWAP_PKT_TYPE_DOT11_MGMT              50
               CAPWAP_PKT_TYPE_DOT11_IAPP            9447
               CAPWAP_PKT_TYPE_DOT11_RFID               0
                CAPWAP_PKT_TYPE_DOT11_RRM               0
              CAPWAP_PKT_TYPE_DOT11_DOT1X               0
         CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE            2191
       CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE               0
             CAPWAP_PKT_TYPE_CAPWAP_CNTRL            7034
              CAPWAP_PKT_TYPE_CAPWAP_DATA               0
          CAPWAP_PKT_TYPE_MOBILITY_CNTRL               0
                         WLS_SMD_WEBAUTH               0
                       SISF_PKT_TYPE_ARP            5292
                      SISF_PKT_TYPE_DHCP             140
                     SISF_PKT_TYPE_DHCP6            1213
                   SISF_PKT_TYPE_IPV6_ND             350
                SISF_PKT_TYPE_DATA_GLEAN              44
             SISF_PKT_TYPE_DATA_GLEAN_V6              51
                SISF_PKT_TYPE_DHCP_RELAY             122
          CAPWAP_PKT_TYPE_CAPWAP_RESERVED               0
```

Configuring DHCP-Required for FlexConnect

Information About FlexConnect DHCP-Required

The DHCP-Required knob on a policy profile forces a connected wireless client to get the IP address from DHCP. When the client completes the DHCP process and acquires an IP address, this IP address is learnt by the controller and only then the client traffic is switched on to the network. The DHCP-Required feature is already supported in central switching.

In Cisco IOS XE Amsterdam 17.2.1, the feature is supported on FlexConnect local switching clients. Prior to Release 17.2.1, DHCP-Required was not enforced on FlexConnect local switching clients. The IP address learnt by the AP or the controller for the wireless client is tracked to create an IP-MAC binding. As part of this feature, when a FlexConnect local switching client roams from one AP to another, the client need not do

the DHCP again in the same L2 network, because the controller tracks the IP address and pushes the binding to the newly roaming AP.

The FlexConnect DHCP-Required feature can be configured from open configuration models, CLI, and from the GUI. The CLI and GUI configurations are described in this chapter. For more information about the open configuration modes, see the https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/172/b_172_programmability_cg.html.

Restrictions and Limitations for FlexConnect DHCP-Required

The following are the restrictions and limitations for the FlexConnect DHCP-Required feature:

- The DHCP-Required feature is applicable for IPv4 addresses only.
- The IP-MAC binding can be pushed to other APs only through the custom policy profile. IP-MAC binding is not available in the default policy. The mapping is propagated to all the APs in the same custom policy profile.
- The DHCP-Required feature works on IP-MAC binding basis and is not supported with third party workgroup bridge (WGB), where WGB wired client information is not shared to AP by the WGB.
- Cisco Wave 2 APs take 180 seconds to remove a client entry with static IP, when DHCP-required is enabled.

Configuring FlexConnect DHCP-Required (GUI)

Perform the steps given below to configure the FlexConnect DHCP-Required feature through the GUI:

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy** window, click the name of the corresponding Policy Profile.
The **Edit Policy Profile** window is displayed.

Step 3 Click the **Advanced** tab.

Step 4 In the **DHCP** section, check the **IPv4 DHCP Required** check box to enable the feature.

Step 5 Click **Update & Apply to Device**.

Configuring FlexConnect DHCP-Required (CLI)

Perform the procedure given below to configure FlexConnect DHCP-Required through the CLI:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device#configure terminal`	
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device#wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)#ipv4 dhcp required`	Enables the FlexConnect DHCP-Required feature.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)#no shutdown`	Saves the configuration.

Verifying FlexConnect DHCP-Required

- To verify the IP address learnt for a client on an IP DHCP-Required policy-enabled WLAN, use the **show wireless client summary** command:

Note The controller or AP does not learn the IP address through other means such as ARP or data gleaning, when IPv4 DHCP-Required is enabled.

```
Device# show wireless client summary
Number of Clients: 1
MAC Address         AP Name           Type  ID  State         Protocol     Method
Role
---------------------------------------------------------------------------------
1cXX.bXXX.59XX      APXXXX.7XXX.4XXX  WLAN  3   IP Learn      11ac         Dot1x
Local
```

- This example shows that the client IP is in the **Run** state, indicating that the client has received the IP address from DHCP:

```
Device# show wireless client summary
Number of Clients: 1
MAC Address       AP Name             Type       ID       State        Protocol
Method      Role
---------------------------------------------------------------------------------
5XXX.37XX.c3XX    APXXXX.4XXX.4XXX    WLAN        3        Run         11n(5)
None        Local
```

CHAPTER 173

Aironet Extensions IE (CCX IE)

- Information About Aironet Extensions Information Element , on page 1937
- Configuring Aironet Extensions IE (GUI), on page 1937
- Configuring Aironet Extensions IE (CLI), on page 1937
- Verifying the Addition of AP Name, on page 1938

Information About Aironet Extensions Information Element

The Cisco Aironet Extensions Information Element (IE) is an attribute used by Cisco devices for better connectivity. It contains information such as the AP name, device type, radio type, AP load, and the number of associated clients, in the beacon and probe responses of the WLAN. The Cisco Client Extensions use this information to associate with the best AP.

The Aironet Extensions IE configuration is disabled by default. With this feature you can set the AP name not through enabling the whole IE extension, but by just inserting just the AP name.

Configuring Aironet Extensions IE (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs** .

Step 2 In the **WLANs** window, click **Add**.

Step 3 In the **Add WLAN** window, under the **Advanced** tab, check the **Aironet IE** check box to enable Aironet IE on the WLAN.

Step 4 Click **Apply to Device**.

Configuring Aironet Extensions IE (CLI)

Perform this procedure to create a WLAN and enable the Aironet Extensions IE feature on the WLAN:

Note For more information about the open configuration models, refer to the Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.1.x.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id* [*ssid*] **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Specifies the WLAN name and ID: • *profile-name*: Profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*: WLAN ID. The range is from 1 to 512. • *ssid*: Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** By default, the WLAN is disabled.
Step 3	**[no] ccx aironet-iesupport** **Example:** `Device(config-wlan)#ccx aironet-iesupport`	Configures the Cisco Client Extensions option and sets the support of Aironet IE on the WLAN. (Use the **no** form of this command to disable the configuration.)

What to do next

1. Create a policy tag. For more information about creating policy tags, refer to *Configuring a Policy Tag (CLI)*.
2. Map the policy tag to the AP. For more information about mapping a policy tag to the AP, refer to *Attaching a Policy Tag and Site Tag to an AP (CLI)*.

Verifying the Addition of AP Name

The following example shows how to verify the addition of the AP Name (using Open Configuration) in the beacon without enabling IE:

```
Device# show wlan id 1
WLAN Profile Name     : wlan-test
================================================
Identifier                                : 1
```

```
Description                                     :
Network Name (SSID)                             : wlan2
Status                                          : Disabled
Broadcast SSID                                  : Enabled
Advertise-Apname                                : Enabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
OKC                                             : Enabled
Number of Active Clients                        : 0
CHD per WLAN                                    : Enabled
WMM                                             : Allowed
Channel Scan Defer Priority:
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
Peer-to-Peer Blocking Action                    : Disabled
```

CHAPTER 174

Device Analytics

- Device Analytics, on page 1941
- Adaptive 802.11r, on page 1945

Device Analytics

Information About Device Analytics

The Device Analytics feature enhances the enterprise Wi-Fi experience for client devices to ensure seamless connectivity. This feature provides a set of data analytics tools for analyzing wireless client device behavior. With device profiling enabled on the controller, information is exchanged between the client device and the controller and AP. This data is encrypted using AES-256-CBC to ensure device security.

Starting from Cisco IOS XE Bengaluru 17.6.1, this feature is supported on Intel devices with AC9560, AC8561, AX201, AX200, AX1650, AX210, AX211, and AX1675 chipsets. Device information and other information received from the Intel devices are shared with Cisco Catalyst Center. It will also be used to enhance device profiling on the controller.

Note From Cisco IOS XE Dublin 17.12.1, MacBook Analytics is supported on the controller when the MacBook device sends 11k action frames along with the model information.

Note Apple clients such as iPhones and iPads use 802.11k action frames to send device information to the controller. When they fail to send 802.11k action frames, the controller will not perform device classification based on the 802.11 protocol. Hence, this falls back to legacy device classification which is based on HTTP and DHCP protocols.

Restrictions for Device Analytics

- This feature is applicable only for Cisco device ecosystem partners.
- This feature is supported only on the 802.11ax and Wave 2 APs.

- This feature is supported using central authentication in either local mode or FlexConnect mode.
- To support Intel devices, AP should have PMF capability and PMF should set to optional or required on the WLAN.

Configuring Device Analytics (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the name of the WLAN.

Step 3 In the **Edit WLAN** window, click the **Advanced** tab.

Step 4 In the **Device Analytics** section, select the **Advertise Support** check box.

Step 5 Select the **Advertise PC Analytics Support** check box to enable PC analytics on the WLAN.

Step 6 (Optional) In the **Device Analytics** section, select the **Share Data with Client** check box.

Step 7 Click **Update & Apply to Device**.

Configuring Device Analytics (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan device_analytics 1 device_analytics`	Enters the WLAN configuration sub-mode. • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. **Note** If you have already configured WLAN, enter **wlan** *wlan-name* command.

	Command or Action	Purpose
Step 3	**client association limit** {*clients-per-wlan* | **ap***clients-per-ap-per-wlan* | **radio** *clients-per-ap-radio-per-wlan*} **Example:** `Device(config)# client association limit 1 1`	Sets the maximum number of clients, clients per AP, or clients per AP radio that can be configured on a WLAN.
Step 4	**[no] device-analytics** **Example:** `Device(config)# device-analytics`	This is enabled by default. Enables or disables device analytics. WLANs advertise analytics capability in beacons & probe responses.
Step 5	**[no] device-analytics** [**export**] **Example:** `Device(config)# device-analytics export`	When **export** option is set, the information from Cisco devices are shared with compatible clients (such as, Samsung devices). Here, information from Cisco devices refer to the Cisco controller details, AP version, and model number. This configuration is disabled by default.
Step 6	**device-analytics pc-analytics** **Example:** `Device(config)# device-analytics pc-analytics`	Enables PC analytics on the WLAN. WLANs advertise analytics capability in beacons & probe responses.
Step 7	**no shutdown** **Example:** `Device(config)# no shutdown`	Enables the WLAN.
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying Device Analytics

Procedure

Step 1 On the **Monitoring > Wireless > Clients** page, click on a client in the table to view its properties and statistics.

Step 2 In the **General** tab, click on **Client Properties** to view the **PC Analytics** reports. This section displays the neighbor AP information, candidate BSSIDs, and reports for low RSSI, beacon miss, failed APs, and unknown APs.

Verifying Device Analytics Configuration

To view the status of device analytics export, use the following command:

```
Device# show wlan 1 test-wlan

WLAN Profile Name     : test-wlan
================================================
Identifier                       : 1
Description                      :
Network Name (SSID)              : test-open-ssid
Status                           : Enabled
Broadcast SSID                   : Enabled
Advertise-Apname                 : Disabled
Universal AP Admin               : Disabled

Device Analytics
    Advertise Support            : Enabled
    Share Data with Client       : Disabled
```

To view client device information, use the following command:

```
Device# show device classifier mac-address 0040.96ae.xxx detail

  Client Mac: 0040.96ae.xxxx
  Device Type: Samsung Galaxy S10e(Phone)
  Confidence Level: 40
  Device Name: android-dhcp-9
  Software Version(Carrier Code): SD7(TMB)
  Device OS: Android 9
  Device Vendor: android-dhcp-9
  Country: US
```

To view the last disconnect reason, use the following command:

```
Device# show device classifier mac-address 0040.96ae.xxxx detail

Client MAC Address : 0040.96ae.xxxx
Client IPv4 Address : 12.1.0.52
Client IPv6 Addresses : fe80::631b:5b4f:f9b6:53cc
Client Username: N/A
AP MAC Address : 7069.5a51.53c0
AP Name: AP4C77.6D9E.61B2
AP slot : 1
Client State : Associated

Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : No/Simple client
Last Disconnect Reason : User initiated disconnection - Device was powered off or Wi-Fi
turned off
```

To view the per client pc-analytics reports, use the following command:

```
Device# show wireless client mac-address 3413.e8b6.xxxx stats pc-analytics

-------------------------
Neighbor APs Info:
-------------------------
Reported time:: 06/21/2021 18:50:34
-------------------------
Roaming Reasons:
```

```
-------------------------
Selected AP RSSI:: -67
Candidate BSSIDs:
-----------------
Neighbor AP RSSI(dB)
a4b2.3903.d10e -70
-------------------------
PC Analytics report stats
-------------------------
----------------------------------------------------------------------
Report Type Processed Reports Dropped Reports
----------------------------------------------------------------------

STA Info 1 0
Neigh AP 1 0
Low RSSI 0 0
Beacon Miss 0 0
Failed AP 0 0
Unknown APs 0 0
```

Adaptive 802.11r

Information About Adaptive 802.11r

The Cisco device ecosystem partner now supports 11r functionality on an adaptive 802.11r SSID. Samsung is one of the partners.

Note The Adaptive 802.11r is enabled by default. This means that when you create a WLAN, the adaptive 802.11r is configured by default.

Client device information such as its model number, supported operating system is shared with the controller and AP while the device receives information such as controller and AP type, software release, etc. Also, this enables 802.11r-compatible devices to benefit from adaptive 802.11r on Cisco networks. This ecosystem comes handy especially for troubleshooting device disconnection from the AP as the controller receives information such as the disconnect reason code from the client device.

Note Devices without 11r support cannot join an SSID where 11r is enabled.

To use the 11r functionality on devices, you need to create a separate SSID with 11r enabled and another with 11r disabled to support the non-11r devices in the network.

Adaptive dot11r is supported by Apple iPad, Apple iPhone, and Samsung S10 devices. However; some software update creates a MIC mismatch error in these devices. But these errors are transient and clients will successfully be able to associate to the SSID in subsequent results.

Configuring Adaptive 802.11r (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the name of the WLAN.

Step 3 In the **Edit WLAN** window, click the **Security** > **Layer2** tab.

Step 4 In the **WPA Parameters** section and **Fast Transition** drop-down list, choose **Adaptive Enabled**.

Step 5 Click **Update & Apply to Device**.

Verifying Adaptive 802.11r

To view the details, use the following command:

```
Device# show running-config all
wlan test-psk 2 test-psk
 security ft adaptive
"adaptive" is  optional
```

Note The following command is used to enable or disable adaptive 11r:

[no] security ft adaptive

The following command is used to enable or disable 802.11r:

[no] security ft

CHAPTER 175

Device Classifier Dynamic XML Support

- Feature History for Device Classifier Dynamic XML Support, on page 1947
- Information About Device Classifier Dynamic XML Support, on page 1948
- Enabling Device Classifier (CLI), on page 1951
- Updating Dynamic XML File, on page 1951
- Verifying TLV Values, on page 1952
- Clearing Old Classification Cache, on page 1952

Feature History for Device Classifier Dynamic XML Support

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 137: Feature History for Device Classifier Dynamic XML Support

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Device Classifier Dynamic XML Support	You can do the following: • Add rules, checks, and profile name to an XML file. • Upload the XML file to the device file system. This feature enables better device classification without upgrading the device to a new release. **Note** Device classifier dynamic XML support is applicable for the following: • Devices that are not classified previously: The classification takes effect from the latest file without any reboot. • Devices that are already classified: The clients have to rejoin for the classification to take effect. • Client previously classified with higher protocol values such as DHCP + HTTP: If the same client wants to be classified with only DHCP, use the **clear wireless client device cache** command.

Information About Device Classifier Dynamic XML Support

The current device classifier uses static XML file wherein you define checks, rules, and profiles based on MAC, DHCP, and HTTP TLVs in wireless devices. The static XML file is converted to a text file and integrated with the image. When you enable the device classified functionality using **device classifier** command, the contents in the text file is read and populated into the device classifier structures.

Note The subsequent device classification is based on the populated device classifier structures.

Presently, if you find any unclassified devices in a controller, the static XML file is updated with the new rules, checks, and profiles to get the devices classified. You will need to wait till the subsequent release as the static XML file is integrated with the image and cannot be changed from the controller.

Workflow: To Classify Unclassified Devices with Dynamic XML File

1. The dynamic XML filename must be **dc_user_profiles.xml**.

Note Files with any other name are not read and parsed even if they have the correct schema.

2. Copy the sample dynamic XML file to your system using the following command:

copy {flash:} {ftp: | tftp:}

3. Provide a new version for the dynamic XML file:

   <Version>1.1</Version>

4. Edit the dynamic XML file with the new rules, checks, and profiles as defined in the schema after examining the TLV values of the unclassified devices.

Note To check the TLV values, use the following command:

show wireless client mac-address *mac* **detail**

5. Copy the dynamic XML file to the device flash using the following command:

   copy {ftp: | tftp:} {flash:}

Once the file is copied to the device file system, the newly connected clients are classified according to the new profiles defined in the dynamic XML file. You need to reconnect the already unclassified devices to send the DHCP and HTTP TLVs, and then classify them according to the new profiles. The already classified devices remain as classified until they are reconnected.

Dynamic XML File

The device classifier dynamic XML support enhancement addresses this problem for device classifier dynamic XML file.

With the introduction of dynamic XML support, you are provided with a new dynamic device classifier XML file support.

Note The filename will be **dc_user_profiles.xml** and you can update the dynamic XML file with the new rules, checks, and profiles based on the devices connected and according to the provided schema.You can then copy this XML file to the device file system to enable better device classification without the need to upgrade the device to a new release.

The static XML file support is still available. If a device is connected, its TLVs are checked with the dynamic XML user profiles first and if it matches it is classified as per that profile. If you search for non-static XML profiles and if it matches it is classified as per that profile.

Note The sample dynamic XML file is available in the device at ***flash:dc_profile_dir/.***. You can consider the following sample dynamic XML file schema and copy this to your system using **copy {flash:} {ftp: | tftp:}** command, and append or replace the content with your own profiles, rules, and checks:

```
<?xml version="1.0" encoding="UTF-8"?>
<DeviceList>
             <CopyRight>Copyright (c) 2021-2022 by Cisco Systems, Inc. All rights
reserved.</CopyRight>
             <Version>1.0</Version>
             <Device>
                   <DeviceType>Sample_Profile_1</DeviceType>
                   <RuleName>Sample_Rule_1</RuleName>
                   <RuleOperator>OR</RuleOperator>
                   <RuleCertaintyMetric>20</RuleCertaintyMetric>
                   <Check>
                              <Protocol>DHCP</Protocol>
                              <TLV-Type>12</TLV-Type>
                              <TLV-Value-Type>String</TLV-Value-Type>
                              <TLV-Value>test</TLV-Value>
                   </Check>
                   <Check>
                              <Protocol>HTTP</Protocol>
                              <TLV-Type>3</TLV-Type>
                              <TLV-Value-Type>Integer</TLV-Value-Type>
                              <TLV-Value>23</TLV-Value>
                    </Check>
             </Device>
             <Device>
                  <DeviceType>Sample_Profile_2</DeviceType>
                  <RuleName>Sample_Rule_2</RuleName>
                  <RuleOperator>AND</RuleOperator>
                  <RuleCertaintyMetric>30</RuleCertaintyMetric>
                  <Check>
                         <Protocol>DHCP</Protocol>
                        <TLV-Type>12</TLV-Type>
                        <TLV-Value-Type></TLV-Value-Type>
                        <TLV-Value>test</TLV-Value>
                  </Check>
                  <Check>
                         <Protocol>MAC</Protocol>
                         <TLV-Value-Type>String</TLV-Value-Type>
                         <TLV-Value>Cisco</TLV-Value>
                   </Check>
</Device>
</DeviceList>
```

Each time you copy a new dynamic XML file, the older user profiles are erased completely and newer profiles are populated. After copying the dynamic XML files, only the newly connected clients are classified based on the new dynamic file whereas the already classified devices still remain as classified with older profiles until they are reconnected.

MAC OUI-Based Profiles

The Organizational Unique Identifier (OUI) of a MAC address is part of the MAC address that identifies the vendor of the network adapter. The OUI is the first three bytes of the six-byte field and administered by the IEEE.

To define MAC-based profiles in the dynamic XML file, see https://standards-oui.ieee.org/.

For example, if the Client MAC address is **7035.094d.000**, then OUI is **0x703509**. You can find the corresponding entry in the https://standards-oui.ieee.org/ as follows:

```
70-35-09   (hex)  Cisco Systems, Inc
703509     (base 16)    Cisco Systems, Inc
      80 West Tasman Drive
      San Jose  CA  94568
      US
```

Enabling Device Classifier (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**device classifier** **Example:** `Device(config)# device classifier`	Enables the classification of attached devices.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Updating Dynamic XML File

To classify a device, add the following lines in the dynamic XML file:

```
<DeviceList>
          <CopyRight>Copyright (c) 2021-2022 by Cisco Systems, Inc. All rights
reserved.</CopyRight>
          <Version>1.1</Version>
          <Device>
                 <DeviceType>Device-test”</DeviceType>
                <RuleName>Rule-Test</RuleName>
               <RuleOperator>AND</RuleOperator>
               <RuleCertaintyMetric>20</RuleCertaintyMetric>
               <Check>
                       <Protocol>DHCP</Protocol>
                       <TLV-Type>12</TLV-Type>
                      <TLV-Value-Type>String</TLV-Value-Type>
                      <TLV-Value>test</TLV-Value>
                </Check>
         </Device>

.............................
</DeviceList>
```

Verifying TLV Values

To verify the TLV values, use the following command:

```
Device# show  wireless  client  mac-address 7035.094d.0001 detail
Client MAC Address : 7035.094d.0001

.....

Nearby AP Statistics:

EoGRE : Pending Classification

Device Classification Information:

  Device Type         : Un-Classified Device

  Device Name      : Unknown Device

  Protocol Map     : 0x000009  (OUI, DHCP)

  Device Protocol  : DHCP                      -→ <Protocol>DHCP</Protocol>

    Type             : 12   14                          --> <TLV-Type>12</TLV-Type>

    Data             : 0e

    00000000  00 0c 00 0a 74 65 73 74  2d 30 30 30 30 31         |....test-00001  |
    ---><TLV-Value>test</TLV-Value>

    Type             : 60   8

    Data             : 08

    00000000  00 3c 00 04 74 65 73 74                           |.<..test        |

    Type             : 55   11

    Data             : 0b

    00000000  00 37 00 07 01 1c 02 03  0f 06 0c                 |.7.........     |

Max Client Protocol Capability: Wi-Fi6 (802.11ax)
```

Clearing Old Classification Cache

If an already classified client uses any of the three type-length-values (TLVs) [OUI, DHCP, or HTTP] and if the combination value is lower, the existing value is ignored. To avoid such a scenario, use the following command:

```
Device# clear wireless client device cache
```

Note The priority of the TLVs is as follows:

- OUI
- DHCP
- HTTP

After executing the clear command, you must rejoin the client to get it classified as per the latest XML file.

CHAPTER 176

BSSID Counters

- BSSID Counters, on page 1955
- Enabling BSSID Statistics and BSSID Neighbor Statistics, on page 1955
- Verifying BSSID Statistics on the Controller, on page 1956

BSSID Counters

This feature helps to retrieve the BSSID statistics when a client is associated with a WLAN for every configured interval. A new configuration is introduced in the controller per AP profile to enable or disable BSSID statistics on the access points. The feature is disabled by default.

Note BSSID counter is not supported on the Cisco Aironet 1800 series APs and Cisco Catalyst 9100 series APs.

Enabling BSSID Statistics and BSSID Neighbor Statistics

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Enters the AP profile configuration submode. *ap-profile-name* is the profile name of the configured AP.
Step 3	**bssid-stats** **Example:** `Device(config-ap-profile)#[no] bssid-stats`	Enables BSSID statistics. Use the **no** form of the command to disable the feature.

	Command or Action	Purpose
Step 4	**bssid-stats bssid-stats-frequency** *bssid-timer-seconds* **Example:** `Device(config-ap-profile)# bssid-stats bssid-stats-frequency 40`	Sets the BSSID stats frequency timer. BSSID statistics frequency timer is in the range of 1 to 180 seconds.
Step 5	**bssid-neighbor-stats** **Example:** `Device(config-ap-profile)# [no] bssid-neighbor-stats`	Enables BSSID neighbor statistics. Use the **no** form of the command to disable the feature.
Step 6	**bssid-neighbor-stats interval** *bssid-interval <1-180>* **Example:** `Device(config-ap-profile)# [no] bssid-neighbor-stats interval 50`	Sets the interval at which BSSID neighbor statistics is sent from the AP. The BSSID neighbor stats interval is in the range of 1to 180 seconds.

Verifying BSSID Statistics on the Controller

To verify the BSSID statistics on the controller, use the following command:

- **show wireless stats ap name** *ap-name* **dot11 24ghz slot** *0* **wlan-id** <*wlan-id*> **statistics**

```
Device# show wireless stats ap name APXXXX.6DXX.58XX dot11 24ghz slot 0 wlan-id 18 stat
BSSID                 : 7069.5a38.112e
WLAN ID               : 18
Client Count          : 1
TX Statistics
---------------------------------------------------------------------------------
Mgmt          Retries      Data Bytes      Data Retries       Subframe Retries
---------------------------------------------------------------------------------
12            18           16081           18                 0
RX Statistics
---------------------------------------------------------------------------------
Mgmt          Data Bytes
---------------------------------------------------------------------------------
74            17693
Data Distribution
---------------------------------------------------------------------------------
Bytes                       RX                          TX
---------------------------------------------------------------------------------
0-64                        55                          93
65-128                      66                          40
129-256                     21                          5
257-512                     10                          3
513-1024                    1                           9
1025-2048                   0                           1
2049-4096                   0                           0
4097-8192                   0                           0
8193-16384                  0                           0
16385-32768                 0                           0
32769-65536                 0                           0
65537-131072                0                           0
131073-262144               0                           0
```

```
262145-524288              0                        0
524289-1048576             0                        0
WMM Statistics
--------------------------------------------------------------------------------
                           RX                       TX
--------------------------------------------------------------------------------
Voice                      0                        43
Video                      0                        0
Best Effort                154                      39
Background                 0                        0
MCS
--------------------------------------------------------------------------------
MCS                        RX                       TX
--------------------------------------------------------------------------------
mcs0                       39                        0
mcs1                       2                         0
mcs2                       5                         0
mcs3                       7                         0
mcs4                       25                        0
mcs5                       59                        0
mcs6                       290                       0
mcs7                       1148                      3
mcs8                       2288                      0
mcs9                       4440                      2
```

- **show ap name** *ap_name* **neighbor summary**

```
Device#show ap name APXXXX.6DXX.59XX neighbor summary

BSSID                 Channel   Channel-width Slot       RSSI              Last-Heard
                          SSID                                      Neighbour

--------------------------------------------------------------------------------------
0008.2f1c.8040        1         20 Mhz       0          -39               03/17/2020
 18:25:14                 aprusty-un-dot1x                          FALSE

0008.2f1c.8041        1         20 Mhz       0          -39               03/17/2020
 18:25:14                 aprusty-sim-11                            FALSE

0008.2f1c.8042        1         20 Mhz       0          -39               03/17/2020
 18:25:14                 one-ph                                    FALSE

0008.2f1c.8044        1         20 Mhz       0          -38               03/17/2020
 18:25:14                 aprusty-test                              FALSE

0008.3296.f340        11        20 Mhz       0          -51               03/18/2020
 10:39:27                 ewlc-ap-dot1x                             FALSE

0008.3296.f341        11        20 Mhz       0          -49               03/18/2020
 10:39:27                 vewlc_small_psk                           FALSE

002a.1022.d950        1         20 Mhz       0          -57               03/17/2020
 18:25:14                 ewlc-ap-dot1x                             FALSE

002a.105c.bfd0        1         20 Mhz       0          -36               03/17/2020
 18:25:14                 ewlc-ap-dot1x                             FALSE

002a.105c.bfd1        1         20 Mhz       0          -37               03/17/2020
 18:25:14                 vewlc_small_psk                           FALSE

002c.c864.76d0        11        20 Mhz       0          -61               03/18/2020
 10:37:37                 rajwlan                                   FALSE


BSSID                 Channel   Channel-width Slot       RSSI              Last-Heard
```

```
                          SSID                                        Neighbour
-----------------------------------------------------------------------------------------------
002c.c8de.59e0        1        20 Mhz       0          -48                 03/17/2020
 18:25:14                 WQ                                          FALSE

002c.c8de.5d80        11       20 Mhz       0          -54                 03/18/2020
 10:39:27                 ewlc-ap-dot1x                               FALSE

002c.c8de.5d81        11       20 Mhz       0          -55                 03/18/2020
 10:39:27                 vewlc_small_psk                             FALSE

002c.c8de.7260        11       20 Mhz       0          -53                 03/18/2020
 10:39:27                 ewlc-ap-dot1x                               FALSE

002c.c8de.7261        11       20 Mhz       0          -54                 03/18/2020
 10:39:27                 vewlc_small_psk                             FALSE

005d.7390.e1e0        1        20 Mhz       0          -54                 03/17/2020
 18:25:14                 rlan                                        FALSE

006b.f114.95a0        1        20 Mhz       0          -60                 03/17/2020
 18:25:14                 zavc                                        FALSE

006b.f114.b0e0        1        20 Mhz       0          -46                 03/17/2020
 18:25:14                 ewlc-ap-dot1x                               FALSE

006c.bc61.2340        1        20 Mhz       0          -63                 03/17/2020
 18:24:44                 dnac-swim                                   FALSE

006c.bc72.5ce0        11       20 Mhz       0          -58                 03/18/2020
 10:39:17                 dnac-swim                                   FALSE
```

CHAPTER 177

Fastlane+

- Information About Fastlane+, on page 1959
- Configuring an Fastlane+ on a WLAN (CLI), on page 1959
- Configuring an Fastlane+ on a WLAN (GUI), on page 1960
- Monitoring Fastlane+, on page 1960
- Verifying Fastlane+, on page 1961

Information About Fastlane+

IEEE 802.11ax allows scheduled access-based uplink transmissions by periodically collecting buffer status reports from clients. The Fastlane+ feature improves the effectiveness of estimating the uplink buffer status for clients, thereby enhancing the user experience for latency-sensitive applications. The Fastlane+ feature can be enabled or disabled on a per-WLAN basis. Support for this feature is indicated in the beacons and probe responses transmitted by an AP.

Note This feature works only if Protected Management Frame (PMF) is configured as optional or mandatory for a WLAN.

Configuring an Fastlane+ on a WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:**	Configures a WLAN and enters WLAN configuration submode.

	Command or Action	Purpose
	`Device(config)# wlan wlan-test 3 ssid-test`	**Note** If you have already configured a WLAN, enter the **wlan** *profile-name* command.
Step 3	**scheduler asr** **Example:** `Device(config-wlan)# scheduler asr`	Configures Fastlane+ feature on a WLAN.

Configuring an Fastlane+ on a WLAN (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > WLANs**.

Step 2 Select a WLAN.

Step 3 Click **Advanced** tab.

Step 4 Check the **Advanced Scheduling Requests Handling** check box to enable the feature on a per-WLAN basis.

Step 5 Click **Update & Apply to Device**.

Monitoring Fastlane+

Procedure

Step 1 Choose **Monitoring >Wireless > Clients**.

Step 2 Click a client name from the client list.

The **Client** window with multiple tabs is activated.

Step 3 Click **General** tab.

Step 4 Click **Client Statistics** tab.

The most recent uplink latency statistics received from the client is displayed in the **Uplink Latency Distribution** section.

Step 5 Click **Client Properties** tab.

The Fastlane+ feature-related client capabilities information is displayed at the bottom of the window.

Verifying Fastlane+

The following example shows how to verify whether Fastlane+ is enabled or disabled for a WLAN:

```
Device# show wlan 2 | include ASR

Advanced Scheduling Requests Handling : Enabled
```

The following example shows how to verify Fastlane+ capability information and the most recent client uplink latency statistics:

```
Device# show wireless client mac-address f45c.89b0.xxxx detail
.
.
.
Regular ASR support: : ENABLED
Non-default Fastlane Profile: : Active
Range Voice Video Background Best-Effort
----------------------------------------------------------------------------------------
[0-20ms] 400 300 200 100
[20-40ms] 401 301 201 101
[40-100ms] 402 302 202 102
[>100ms] 403 303 203 103
```

The following example shows how to verify Fastlane+ statistics along with Fastlane+ capability and uplink latency statistics for all the Fastlane+ clients on a WLAN.

Note **show interfaces dot11radio asr-info all** is an AP command, and does not work on the controller.

```
Device# show interfaces Dot11Radio 1 asr-info all

[*10/12/2020 18:45:21.0149]
[*10/12/2020 18:45:21.0150]  Client-MAC:[26:52:CF:C8:D0:1C] AID:[3] ASR-Capability:[0x1]
[*10/12/2020 18:45:21.0150]  BE- LAT[0-20]:[267] LAT[20-40]:[57] LAT[40-100]:[32]
LAT[>100]:[26]
[*10/12/2020 18:45:21.0150]  BK- LAT[0-20]:[0] LAT[20-40]:[0] LAT[40-100]:[0] LAT[>100]:[0]
[*10/12/2020 18:45:21.0150]  VI- LAT[0-20]:[0] LAT[20-40]:[0] LAT[40-100]:[0] LAT[>100]:[0]
[*10/12/2020 18:45:21.0150]  VO- LAT[0-20]:[2222] LAT[20-40]:[409] LAT[40-100]:[224]
LAT[>100]:[163]
[*10/12/2020 18:45:21.0150]
[*10/12/2020 18:45:21.0206] HTT_PEER_DETAILS_TLV:
[*10/12/2020 18:45:21.0206] peer_type = 0
[*10/12/2020 18:45:21.0206] sw_peer_id = 98
[*10/12/2020 18:45:21.0206] vdev_id = 25
[*10/12/2020 18:45:21.0206] pdev_id = 0
[*10/12/2020 18:45:21.0206] ast_idx = 1187
[*10/12/2020 18:45:21.0206] mac_addr = 26:52:cf:c8:d0:1c
[*10/12/2020 18:45:21.0206] peer_flags = 0x200006f9
[*10/12/2020 18:45:21.0206] qpeer_flags = 0x8
[*10/12/2020 18:45:21.0206]
[*10/12/2020 18:45:21.0206] HTT_STATS_PEER_ASR_STATS_TLV
[*10/12/2020 18:45:21.0206] asr_bmap: 0x8
[*10/12/2020 18:45:21.0206] asr_muedca_update_cnt: 1
[*10/12/2020 18:45:21.0206] asr_muedca_reset_cnt: 1
[*10/12/2020 18:45:21.0206] asr_ul_mu_bsr_trigger: 2376
[*10/12/2020 18:45:21.0206] asr_min_trig_intv- BE:0         BK:0 VI:0 VO:19
[*10/12/2020 18:45:21.0206] asr_max_trig_intv- BE:0         BK:0 VI:0 VO:20
[*10/12/2020 18:45:21.0207] asr_min_alloc_rate- BE:0         BK:0 VI:0 VO:12
[*10/12/2020 18:45:21.0207] asr_ul_su_data_ppdu_cnt- BE:0         BK:0 VI:0 VO:2149
```

```
[*10/12/2020 18:45:21.0207] asr_ul_su_data_ppdu_bytes- BE:0         BK:0 VI:0 VO:757546
[*10/12/2020 18:45:21.0207] asr_ul_mu_trig_ppdu_cnt- BE:0         BK:0 VI:0 VO:5002
[*10/12/2020 18:45:21.0207] asr_ul_mu_trig_ppdu_bytes- BE:0         BK:0 VI:0 VO:2400960
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_ppdu_cnt- BE:0         BK:0 VI:0 VO:2134
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_ppdu_bytes- BE:0         BK:0 VI:0 VO:736578
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_padding_bytes- BE:0         BK:0 VI:0 VO:2953488
```

The following examples show how to verify scheduling statistics along with capability and uplink latency statistics for a given client on a WLAN:

Note The **show interfaces dot11radio asr-info** is an AP command and it will not work on the controller.

```
Device# show interfaces Dot11Radio 1 asr-info 26:XX:CF:XX:D0:XX

[*10/12/2020 18:45:21.0149]
[*10/12/2020 18:45:21.0150]  Client-MAC:[26:52:CF:C8:D0:1C] AID:[3] ASR-Capability:[0x1]
[*10/12/2020 18:45:21.0150]  BE- LAT[0-20]:[267] LAT[20-40]:[57] LAT[40-100]:[32]
LAT[>100]:[26]
[*10/12/2020 18:45:21.0150]  BK- LAT[0-20]:[0] LAT[20-40]:[0] LAT[40-100]:[0] LAT[>100]:[0]
[*10/12/2020 18:45:21.0150]  VI- LAT[0-20]:[0] LAT[20-40]:[0] LAT[40-100]:[0] LAT[>100]:[0]
[*10/12/2020 18:45:21.0150]  VO- LAT[0-20]:[2222] LAT[20-40]:[409] LAT[40-100]:[224]
LAT[>100]:[163]
[*10/12/2020 18:45:21.0150]
[*10/12/2020 18:45:21.0206] HTT_PEER_DETAILS_TLV:
[*10/12/2020 18:45:21.0206] peer_type = 0
[*10/12/2020 18:45:21.0206] sw_peer_id = 98
[*10/12/2020 18:45:21.0206] vdev_id = 25
[*10/12/2020 18:45:21.0206] pdev_id = 0
[*10/12/2020 18:45:21.0206] ast_idx = 1187
[*10/12/2020 18:45:21.0206] mac_addr = 26:xx:cf:xx:d0:xx
[*10/12/2020 18:45:21.0206] peer_flags = 0x200006f9
[*10/12/2020 18:45:21.0206] qpeer_flags = 0x8
[*10/12/2020 18:45:21.0206]
[*10/12/2020 18:45:21.0206] HTT_STATS_PEER_ASR_STATS_TLV
[*10/12/2020 18:45:21.0206] asr_bmap: 0x8
[*10/12/2020 18:45:21.0206] asr_muedca_update_cnt: 1
[*10/12/2020 18:45:21.0206] asr_muedca_reset_cnt: 1
[*10/12/2020 18:45:21.0206] asr_ul_mu_bsr_trigger: 2376
[*10/12/2020 18:45:21.0206] asr_min_trig_intv- BE:0         BK:0 VI:0 VO:19
[*10/12/2020 18:45:21.0206] asr_max_trig_intv- BE:0         BK:0 VI:0 VO:20
[*10/12/2020 18:45:21.0207] asr_min_alloc_rate- BE:0         BK:0 VI:0 VO:12
[*10/12/2020 18:45:21.0207] asr_ul_su_data_ppdu_cnt- BE:0         BK:0 VI:0 VO:2149
[*10/12/2020 18:45:21.0207] asr_ul_su_data_ppdu_bytes- BE:0         BK:0 VI:0 VO:757546
[*10/12/2020 18:45:21.0207] asr_ul_mu_trig_ppdu_cnt- BE:0         BK:0 VI:0 VO:5002
[*10/12/2020 18:45:21.0207] asr_ul_mu_trig_ppdu_bytes- BE:0         BK:0 VI:0 VO:2400960
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_ppdu_cnt- BE:0         BK:0 VI:0 VO:2134
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_ppdu_bytes- BE:0         BK:0 VI:0 VO:736578
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_padding_bytes- BE:0         BK:0 VI:0 VO:2953488
```

CHAPTER 178

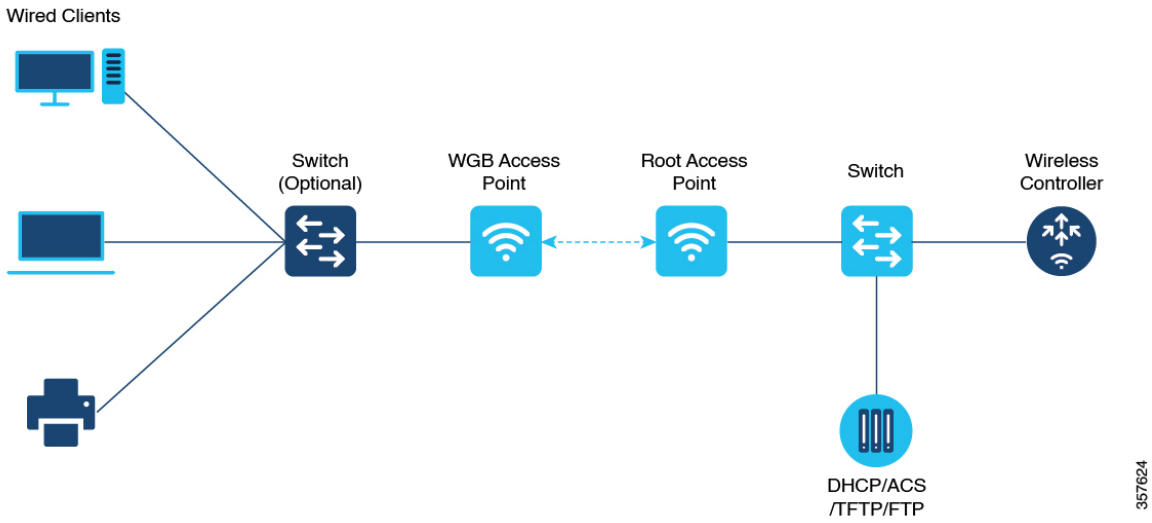
Workgroup Bridges

- Cisco Workgroup Bridges, on page 1963
- Configuring Workgroup Bridge on a WLAN, on page 1966
- Verifying the Status of a Workgroup Bridge on the Controller, on page 1968
- Configuring Access Points as Workgroup Bridge, on page 1968
- Information About Simplifying WGB Configuration, on page 1983
- Configuring Multiple WGBs (CLI), on page 1984
- Verifying WGB Configuration, on page 1984

Cisco Workgroup Bridges

A workgroup bridge (WGB) is an Access Point (AP) mode to provide wireless connectivity to wired clients that are connected to the Ethernet port of the WGB AP. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the WLC through infrastructure AP using Internet Access Point Protocol (IAPP) messaging. The WGB establishes a single wireless connection to the root AP, which in turn, treats the WGB as a wireless client.

Figure 53: Example of a WGB



Starting from Cisco IOS XE Cupertino 17.8.1, WGB is supported on the following Cisco Catalyst 9100 Series Access Points.

- Cisco Catalyst 9105
- Cisco Catalyst 9115
- Cisco Catalyst 9120

Starting from Cisco IOS XE Dublin 17.10.1, WGB is supported on the following Cisco Catalyst 9100 Series Access Points.

- Cisco Catalyst 9124
- Cisco Catalyst 9130

From Cisco IOS XE Cupertino 17.9.1 onwards, WGB supports one radio for uplink (backhaul) connectivity and another radio for serving wireless clients. This feature is supported on the Cisco 11AX APs such as Cisco Catalyst 9105 APs, Cisco Catalyst 9115 APs, Cisco Catalyst 9120 APs.

OPEN and PSK security (WPA2 Personal) based wireless clients can be associated to WGB independent of its uplink connectivity, but they will not be able to pass traffic unless WGB has uplink connectivity. Radius server must be configured and the WGB should have uplink connectivity for authentication of wireless clients to 802.1x security (WPA2 Enterprise) WLAN. Both IPv4 and IPv6 traffic forwarding is supported for wireless clients. Static IP and Passive Client support is enabled by default on these WLANs.

The following features are supported for use with a WGB:

Table 138: WGB Feature Matrix

Feature	Cisco Wave 1 APs	Cisco Wave 2 and 11AX APs
802.11r	Supported	Supported
QOS	Supported	Supported
UWGB mode	Supported	Supported on Wave 2 APs Not supported on 11AX APs
IGMP Snooping or Multicast	Supported	Supported
802.11w	Supported	Supported
PI support (without SNMP)	Supported	Not supported
IPv6	Supported	Supported
VLAN	Supported	Supported
802.11i (WPAv2)	Supported	Supported
Broadcast tagging/replicate	Supported	Supported
Unified VLAN client	Implicitly supported (No CLI required)	Supported
WGB client	Supported	Supported

Feature	Cisco Wave 1 APs	Cisco Wave 2 and 11AX APs
802.1x – PEAP, EAP-FAST, EAP-TLS	Supported	Supported
NTP	Supported	Supported
Wired client support on all LAN ports	Supported in Wired-0 and Wired-1 interfaces	Supported in all Wired-0, 1 and LAN ports 1, 2, and 3
Second radio wireless client support	Supported	Supported on Cisco 11AX APs only.

The following table shows the supported and unsupported authentication and switching modes for Cisco APs when connecting to a WGB.

Note Workgroup Bridge mode is supported on the WiFi6 Pluggable Module from Cisco IOS XE Bengaluru 17.6.1.

Table 139: Supported Access Points and Requirements

Access Points	Requirements
Cisco Aironet 2700, 3700, and 1572 Series	Requires autonomous image.
Cisco Aironet 2800, 3800, 4800, 1562, and Cisco Catalyst 9105, 9115, 9120, 9124, and 9130, IW6300 and ESW6300 Series	CAPWAP image starting from Cisco AireOS 8.8 release.

Table 140: WGB Support on APs

WGB WLAN Support	Cisco Wave 2 APs	Cisco Catalyst 9100 Series APs
Central Authentication	Supported	Supported
Central Switching	Supported	Supported
Local Authentication	Not Supported	Not Supported
Local Switching	Supported	Supported

- MAC filtering is not supported for wired clients.
- Idle timeout is not supported for both WGB and wired clients.
- Session timeout is not applicable for wired clients.
- Web authentication is not supported.
- The total number of clients supported by WGB (wired + wireless) is limited to 20 clients.
- If you want to use a chain of certificates, copy all the CA certificates to a file and install it under a trust point on the WGB, else server certificate validation may fail.

- Wired clients connected to a WGB inherit the WGB's QoS and AAA override attributes.
- To enable the WGB to communicate with the root AP, create a WLAN and make sure that Aironet IE is enabled under the Advanced settings.
- WPA2 Enterprise security works only if the uplink WLAN is enabled for FlexConnect local switching or Fabric enabled WLAN.
- Radius override is not supported for wireless clients that are associated with WGB WLANs.
- WGB does not support dot1x wired client authentication when used with power injector.

  The power-injector drops all EAPOL packets received from the wired client and does not forward it to the WGB's wired0 interface. In such cases, use PoE plus hub behind the wired0 interface and connect the wired clients to the hub.
- After WGB reload, the WGB dot1x wired clients behind a hub do not trigger authentication automatically, unless done manually.

  After WGB is reloaded the WGB dot1x wired clients which are behind a hub remain authenticated or connected on their side and do not get notified that the WGB is reloaded. Clients are also not shown on the WGB bridge table. The client interfaces must be manually disabled and enabled back to trigger authentication.
- When the dot1x wired client Ethernet interface is disabled and then enabled again, client authentication might fail for some of dot1x wired clients, at times.

Configuring Workgroup Bridge on a WLAN

Follow the procedure given below to configure a WGB on a WLAN:

For WGB to join a wireless network there are specific settings on the WLAN and on the related policy profile.

Note For the configuration given below, it is assumed that the WLAN security is already configured.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan WGB_Test`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**ccx aironet-iesupport** **Example:** `Device(config-wlan)# ccx aironet-iesupport`	Configures the Cisco Client Extensions option and sets the support of Aironet IE on the WLAN.
Step 4	**exit** **Example:** `Device(config-wlan)# exit`	Exits the WLAN configuration submode.
Step 5	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy test-wgb`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 6	**description** *description* **Example:** `Device(config-wireless-policy)# description "test-wgb"`	Adds a description for the policy profile.
Step 7	**vlan** *vlan-no* **Example:** `Device(config-wireless-policy)# vlan 48`	Assigns the profile policy to the VLAN.
Step 8	**wgb vlan** **Example:** `Device(config-wireless-policy)# wgb vlan`	Configures WGB VLAN client support.
Step 9	**wgb broadcast-tagging** **Example:** `Device(config-wireless-policy)# wgb broadcast-tagging`	Configures WGB broadcast tagging on a WLAN.
Step 10	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Restarts the policy profile.
Step 11	**exit** **Example:** `Device(config-wireless-policy)# exit`	Exits the wireless policy configuration mode.
Step 12	**wireless tag policy** *policy-tag* **Example:** `Device(config)# wireless tag policy WGB_Policy`	Configures policy tag and enters policy tag configuration mode.

	Command or Action	Purpose
Step 13	**wlan** *profile-name* **policy** *profile-policy* **Example:** `Device(config-policy-tag)# wlan WGB_Test policy test-wgb`	Maps a policy profile to a WLAN profile.
Step 14	**end** **Example:** `Device(config-policy-tag)# end`	Exits policy tag configuration mode, and returns to privileged EXEC mode.

Verifying the Status of a Workgroup Bridge on the Controller

Use the following commands to verify the status of a WGB.

To display the wireless-specific configuration of active clients, use the following command:

```
Device# show wireless client summary
```

To display the WGBs on your network, use the following command:

```
Device# show wireless wgb summary
```

To display the details of wired clients that are connected to a particular WGB, use the following command:

```
Device# show wireless wgb mac-address 00:0d:ed:dd:25:82 detail
```

Configuring Access Points as Workgroup Bridge

Turning Cisco Aironet 2700/3700/1572 Series AP into Autonomous Mode

Before you begin

Download the autonomous image for the specific access point from software.cisco.com and place it on a TFTP server.

Procedure

	Command or Action	Purpose
Step 1	**debug capwap console cli** **Example:** `Device# debug capwap console cli`	Enables the console CLI.
Step 2	**archive download-sw force-reload overwrite tftp:***ipaddress filepath filename* **Example:**	Downloads the autonomous image to the access point.

	Command or Action	Purpose
	`Device(config)# archive download-sw force-reload overwrite tftp://10.10.10.1/tftp/c1800.tar`	

Configuring Cisco Wave 2 APs or 11AX APs in Workgroup Bridge or CAPWAP AP Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters in to the privileged mode of the AP.
Step 2	**ap-type workgroup-bridge** **Example:** `Device# ap-type workgroup-bridge`	Moves the AP in to the Workgroup Bridge mode.

Step 3	**configure ap address ipv4 dhcp** or **configure ap address ipv4 static***ip-address netmask gateway-ipaddress*
	Example:
	DHCP IP Address
	`Device# configure ap address ipv4 dhcp`
	Static IP Address
	`Device# configure ap address ipv4 static 10.10.10.2 255.255.255.234 192.168.4.1`
		Configures DHCP or Static IP address.

Step 4	**configure ap management add username** *username* **password** *password* **secret** *secret* **Example:** `Device# configure ap management add username xyz-user password ****** secret cisco`	Configures an username for the AP management.
Step 5	**configure ap hostname***host-name* **Example:** `Device# configure ap hostname xyz-host`	Configures the AP hostname.

Configure an SSID Profile for Cisco Wave 2 and 11AX APs (CLI)

This procedure is an AP procedure. The CLIs listed in the procedure given below work only on the AP console and not on the controller.

Procedure

	Command or Action	Purpose

Step 1	**configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication** {**open** | **psk** *preshared-key* **key-management** {**dot11r** | **wpa2** | **dot11w** |{**optional** | **required** }}| **eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w**|{**optional** | **required**}}
	Example:
	SSID profile with open authentication.
	`Device# configure ssid-profile test WRT s1 authentication open`
	SSID profile with PSK authentication.
	`Device# configure ssid-profile test WRT s1 authentication psk 1234 key-management dot11r optional`
	SSID profile with EAP authentication.
	`Device# configure ssid-profile test WRT s1 authentication eap profile test2 key-management dot11r optional`
		Choose an authentication protocol (Open, PSK, or EAP) for the SSID profile.

Step 2	**configure dot11radio** *radio-interface* **mode wgb ssid-profile** *profle-name* **Example:** `Device# configure dot11radio r1 mode wgb ssid-profile doc-test`	Attaches an SSID profile to a radio interface.
Step 3	**configure ssid-profile** *profile-name* **ssid** *ssid-name* **dtim-period** *value in beacon intervals* **Example:** `Device# configure ssid-profile test ssid s1 dtim-period 50`	Configures the DTIM period. **Note** This command is supported for wireless clients from Cisco IOS XE Cupertino 17.9.1 onwards.
Step 4	**configure qos profile** *qos-profile-name* {**bronze** | **gold** | **platinum** | **silver**} **Example:** `Device# configure qos profile qos-profile gold`	Creates a gold QoS profile.
Step 5	**configure ssid-profile** *profile-name* **ssid** *ssid-name* **qos profile** *qos-profile-name* **Example:** `Device# configure ssid-profile test ssid s1 qos profile qos-profile`	Maps the QoS profile to the SSID profile. **Note** This command is supported for wireless clients from Cisco IOS XE Cupertino 17.9.1 onwards.

	Command or Action	Purpose
Step 6	**configure ssid-profile** *profle-name* **delete** **Example:** `Device# configure ssid-profile doc-test delete`	(Optional) Deletes an SSID profile.
Step 7	**show wgb ssid** **Example:** `Device# show wgb ssid`	(Optional) Displays summary of configured and connected SSIDs.
Step 8	**show wgb packet statistics** **Example:** `Device# show wgb packet statistics`	(Optional) Displays management, control, and data packet statistics.

Configuring the Authentication Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure radius authentication <primary | secondary> add <ipv4|ipv6> address** *radius-server-ip-address* **port** *radius-server-port-number* **secret** *radius-secret* **Example:** `Device# configure radius authentication primary add ipv4 192.168.1.2 port 1812 secret Cisco123`	Configures a primary and (or) secondary radius server with an IPv4 or IPv6 IP, port, and secret.

Configuring a Dot1X Credential (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure dot1x credential** *profile-name* **username** *name* **password** *password* **Example:** `Device# configure dot1x credential test1 username XYZ password *****`	Configures a dot1x credential.
Step 2	**configure dot1x credential** *profile-name* **delete** **Example:** `Device# configure dot1x credential test1 delete`	Removes a dot1x profile.

	Command or Action	Purpose
Step 3	**clear wgb client** {**all** | **single** *mac-addr* } **Example:** `Device# clear wgb client single xxxx.xxxx.xxxx.xxxx`	Deauthenticates a WGB client.

Configuring an EAP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure eap-profile** *profile-name* **method** {**fast** | **leap** | **peap** | **tls**} **Example:** `Device# configure eap-profile test-eap method fast`	Configures an EAP profile.

Step 2	**configure eap-profile** *profile-name* **trustpoint default** or **configure eap-profile** *profile-name* **trustpoint name** *trustpoint-name*
	Example:
	EAP Profile to Trustpoint with MIC Certificate.
	`Device# configure eap-profile test-eap trustpoint default`
	EAP Profile to Trustpoint with CA Certificate.
	`Device# configure eap-profile test-eap trustpoint cisco`
		Configures an EAP profile with a trustpoint.

Step 3	**configure eap-profile** *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*} **Example:** `Device# configure eap-profile test-eap trustpoint default`	Attaches the CA trustpoint. **Note** With the default profile, WGB uses the internal MIC certificate for authentication.
Step 4	**configure eap-profile** *profile-name* **dot1x-credential** *profile-name* **Example:** `Device# configure eap-profile test-eap dot1x-credential test-profile`	Configures the 802.1X credential profile.
Step 5	**configure eap-profile** *profile-name* **delete** **Example:** `Device# configure eap-profile test-eap delete`	(Optional) Deletes an EAP profile.

	Command or Action	Purpose
Step 6	**show wgb eap dot1x credential profile** **Example:** `Device# show wgb eap dot1x credential profile`	(Optional) Displays the WGB EAP dot1x profile summary.
Step 7	**show wgb eap profile** **Example:** `Device# show wgb eap profile`	(Optional) Displays the EAP profile summary.
Step 8	**show wgb eap profile all** **Example:** `Device# show wgb eap profile all`	(Optional) Displays the EAP and dot1x profiles.

Configuring Manual-Enrollment of a Trustpoint for Workgroup Bridge (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure crypto pki trustpoint** *ca-server-name* **enrollment terminal** **Example:** `Device# configure crypto pki trustpoint ca-server-US enrollment terminal`	Configures a trustpoint in WGB.
Step 2	**configure crypto pki trustpoint** *ca-server-name* **authenticate** **Example:** `Device# configure crypto pki trustpoint ca-server-US authenticate`	Authenticates a trustpoint manually. Enter the base 64 encoded CA certificate and end the certificate by entering **quit** in a new line.
Step 3	**configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* **Example:** `Device# configure crypto pki trustpoint ca-server-Us key-size 60`	Configures a private key size.
Step 4	**configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code* |*state-name* |*locality* |*org-name* |*org-unit* |*email*] **Example:**	Configures the subject name.

	Command or Action	Purpose
	`Device# configure crypto pki trustpoint ca-server-US subject-name test US CA abc cisco AP test@cisco.com`	
Step 5	**configure crypto pki trustpoint** *ca-server-name* **enrol** **Example:** `Device# configure crypto pki trustpoint ca-server-US enroll`	Generates a private key and Certificate Signing Request (CSR). Afterwards, create the digitally signed certificate using the CSR output in the CA server.
Step 6	**configure crypto pki trustpoint** *ca-server-name* **import certificate** **Example:** `Device# configure crypto pki trustpoint ca-server-US import certificate`	Import the signed certificate in WGB. Enter the base 64 encoded CA certificate and end the certificate by using **quit** command in a new line.
Step 7	**configure crypto pki trustpoint** *ca-server-name* **delete** **Example:** `Device# configure crypto pki trustpoint ca-server-US delete`	(Optional) Delete a trustpoint.
Step 8	**show crypto pki trustpoint** **Example:** `Device# show crypto pki trustpoint`	(Optional) Displays the trustpoint summary.
Step 9	**show crypto pki trustpoint** *trustpoint-name* **certificate** **Example:** `Device# show crypto pki trustpoint ca-server-US certificate`	(Optional) Displays the content of the certificates that are created for a trustpoint.

Configuring Auto-Enrollment of a Trustpoint for Workgroup Bridge (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url* **Example:** `Device# configure crypto pki trustpoint`	Enrolls a trustpoint in WGB using the server URL.

	Command or Action	Purpose
	`ca-server-US enrollment url https://cisco/certsrv`	
Step 2	**configure crypto pki trustpoint** *ca-server-name* **authenticate** **Example:** `Device# configure crypto pki trustpoint ca-server-US authenticate`	Authenticates a trustpoint by fetching the CA certificate from CA server automatically.
Step 3	**configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* **Example:** `Device# configure crypto pki trustpoint ca-server-Us key-size 60`	Configures a private key size.
Step 4	**configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code* |*state-name* |*locality* |*org-name* |*org-unit* |*email*] **Example:** `Device# configure crypto pki trustpoint ca-server-US subject-name test US CA abc cisco AP test@cisco.com`	Configures the subject name.
Step 5	**configure crypto pki trustpoint** *ca-server-name* **enrol l** **Example:** `Device# configure crypto pki trustpoint ca-server-US enroll`	Enrolls the trustpoint. Request the digitally signed certificate from the CA server.
Step 6	**configure crypto pki trustpoint** *ca-server-name* **auto-enroll enable** *renew-percentage* **Example:** `Device# configure crypto pki trustpoint ca-server-US auto-enroll enable  10`	Enables auto-enroll of the trustpoint. You can disable auto-enrolling by using the **disable** option in the command.
Step 7	**configure crypto pki trustpoint***trustpoint-name* **delete** **Example:** `Device# configure crypto pki trustpoint ca-server-US delete`	(Optional) Deletes a trustpoint.

	Command or Action	Purpose
Step 8	**show crypto pki trustpoint** **Example:** `Device# show crypto pki trustpoint`	(Optional) Displays the trustpoint summary.
Step 9	**show crypto pki trustpoint***trustpoint-name* **certificate** **Example:** `Device# show crypto pki trustpoint ca-server-US certificate`	(Optional) Displays the content of the certificates that are created for a trustpoint.
Step 10	**show crypto pki timers** **Example:** `Device# show crypto pki timers`	(Optional) Displays the PKI timer information.

Configuring Manual Certificate Enrolment Using TFTP Server (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *addr/file-name* **Example:** `Device# configure crypto pki trustpoint ca-server-US enrollment tftp://10.8.0.6/all_cert.txt`	Specifies the enrolment method to retrieve the CA certificate and client certificate for a trustpoint in WGB.
Step 2	**configure crypto pki trustpoint** *ca-server-name* **authenticate** **Example:** `Device# configure crypto pki trustpoint ca-server-US authenticate`	Retrieves the CA certificate and authenticates it from the specified TFTP server. If the file specification is included, the wgb will append the extension ".ca" to the specified filename.
Step 3	**configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* **Example:** `Device# configure crypto pki trustpoint ca-server-Us key-size 60`	Configures a private key size.
Step 4	**configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* [*2ltr-country-code* |*state-name* |*locality* |*org-name* |*org-unit* |*email*]	Configures the subject name.

	Command or Action	Purpose

	Example:
	`Device# configure crypto pki trustpoint`
	
	`ca-server-US subject-name test US CA abc cisco AP test@cisco.com`	

Step 5	**configure crypto pki trustpoint** *ca-server-name* **enrol**
	Example:
	`Device# configure crypto pki trustpoint`
	
	`ca-server-US enroll`
		Generate a private key and Certificate Signing Request (CSR) and writes the request out to the TFTP server. The filename to be written is appended with the extension ".req".

Step 6	**configure crypto pki trustpoint** *ca-server-name* **import certificate**
	Example:
	`Device# configure crypto pki trustpoint`
	
	`ca-server-US import certificate`
		Import the signed certificate in WGB using TFTP at the console terminal, which retrieves the granted certificate.
		The WGB will attempt to retrieve the granted certificate using TFTP using the same filename and the file name append with ".crt" extension.

Step 7	**show crypto pki trustpoint** **Example:** `Device# show crypto pki trustpoint`	(Optional) Displays the trustpoint summary.
Step 8	**show crypto pki trustpoint** *trustpoint-name* **certificate** **Example:** `Device# show crypto pki trustpoint ca-server-US certificate`	(Optional) Displays the content of the certificates that are created for a trustpoint.

Importing the PKCS12 Format Certificates from the TFTP Server (CLI)

Procedure

	Command or Action	Purpose

Step 1	**configure crypto pki trustpoint** *ca-server-name* **import pkcs12 tftp** *addr/file-name* **password** *pwd*
	Example:
	`Device# configure crypto pki trustpoint`
	
	`ca-server-US enrollment tftp://10.8.0.6/all_cert.txt password ******`
		Imports PKCS12 format certificate from the TFTP server.

Step 2	**show crypto pki trustpoint** **Example:**	(Optional) Displays the trustpoint summary.

	Command or Action	Purpose
	`Device# show crypto pki trustpoint`	
Step 3	**show crypto pki trustpoint** *trustpoint-name* **certificate** **Example:** `Device# show crypto pki trustpoint ca-server-US certificate`	(Optional) Displays the content of the certificates that are created for a trustpoint.

Configuring Radio Interface for Workgroup Bridges (CLI)

From the available two radio interfaces, before configuring WGB or UWGB mode on one radio interface, configure the other radio interface to root AP mode.

Procedure

	Command or Action	Purpose
Step 1	**configure dot11radio** *radio-int* **mode root-ap** **Example:** `Device# configure dot11Radio 0/3/0 mode root-ap`	Maps a radio interface as root AP. **Note** When an active SSID or EAP profile is modified, you need to reassociate the profile to the radio interface for the updated profile to be active.
Step 2	**configure dot11Radio <0|1> wlan add** *ssid-profile-name ssid-number* **Example:** `Device# configure dot11radio 1 wlan add ssid-profile-name ssid-number`	Configures the WLAN at the root AP mode radio. Enter the SSID profile name and SSID number between 1 and 16.
Step 3	**configure dot11Radio <0|1> wlan delete** *ssid-profile-name* **Example:** `Device# configure dot11radio 1 wlan delete ssid-profile-name`	Deletes WLAN from the radio configuration. Enter the SSID profile name.
Step 4	**configure dot11Radio <0|1> channel** *channel-number width* **Example:** `Device# configure dot11radio 1 channel 36 80`	Configures a radio channel to broadcast the SSID. The channel numbers are between 1 and 173. The channel width values are 20, 40, 80, and 160.

	Command or Action	Purpose
		Note • Only 20MHz channel width is supported on radio 0 (2.4-GHz band). • If radar is detected on a configured channel on radio 1, then the channel automatically changes to a non-DFS channel with a channel width of 20MHz. The administrator must reset the radio to bring it back to the configured channel.
Step 5	**configure dot11Radio <0|1> beacon-period** *beacon-interval* **Example:** `Device# configure dot11radio 1 beacon-period 120`	Configures the periodic beacon interval in milli-seconds. The value range is between 2 and 2000 milli-seconds.
Step 6	**configure dot11Radio** *radio-int* **mode wgb ssid-profile** *ssid-profile-name* **Example:** `Device# configure dot11Radio 0/3/0 mode wgb ssid-profile bgl18`	Maps a radio interface to a WGB SSID profile.
Step 7	**configure dot11Radio** *radio-int* **mode uwgb** *mac-addr* **ssid-profile** *ssid-profile-name* **Example:** `Device# configure dot11Radio 0/3/0 mode uwgb 0042.5AB6.0EF0 ssid-profile bgl18`	Maps a radio interface to a WGB SSID profile.
Step 8	**configure dot11Radio** *radio-int* {**enable**| **disable**} **Example:** `Device# configure dot11Radio 0/3/0 mode enable`	Configures a radio interface. **Note** After configuring the uplink to the SSID profile, we recommend that you disable and enable the radio for the changes to be active.
Step 9	**configure dot11Radio** *radio-int* **antenna** {**a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**} **Example:** `Device# configure dot11Radio 0/3/0 antenna a-antenna`	Configures a radio antenna.
Step 10	**configure dot11Radio** *radio-int* **encryption mode ciphers aes-ccm** {	Configures the radio interface.

	Command or Action	Purpose
	Example: `Device# configure dot11Radio radio-int encryption mode ciphers aes-ccm`	
Step 11	**configure wgb mobile rate** {**basic 6 9 18 24 36 48 54** | **mcs** *mcs-rate*} **Example:** `Device# configure wgb mobile rate basic 6 9 18 24 36 48 54`	Configures the device channel rate.
Step 12	**configure wgb mobile period** *secondsthres-signal* **Example:** `Device# configure wgb mobile period 30 -50`	Configure the threshold duration and signal strength to trigger scanning.
Step 13	**configure wgb mobile station interface dot11Radio** *radio-int* **scan** *channel-number* **add** **Example:** `Device# configure wgb mobile station interface dot11Radio 0/3/0 scan 2 add`	Configures the static roaming channel.
Step 14	**configure wgb mobile station interface dot11Radio** *radio-int* **scan** *channel-number* **delete** **Example:** `Device# configure wgb mobile station interface dot11Radio 0/3/0 scan 2 delete`	(Optional) Delete the mobile channel.
Step 15	**configure wgb mobile station interface dot11Radio** *radio-int* **scan disable** **Example:** `Device# configure wgb mobile station interface dot11Radio 0/3/0 scan disable`	(Optional) Disable the mobile channel.
Step 16	**configure wgb beacon miss-count** *value* **Example:** `Device# configure wgb beacon miss-count 12`	(Optional) Configure the beacon miss-count. By default, this is set to disabled. **Note** When you set the beacon miss-count value to 10 or lower, then the beacon miss-count gets disabled. Set the value to 11 or higher to enable this function.

	Command or Action	Purpose
Step 17	**show wgb wifi** *wifi-interface* **stats** **Example:** `Device# show wgb wifi 0/3/0 stats`	(Optional) Displays the Wi-Fi station statistics.
Step 18	**show controllers dot11Radio** *radio-interface* **antenna** **Example:** `Device# show controllers dot11Radio 0/3/0 antenna`	(Optional) Displays the radio antenna statistics.
Step 19	**show wgb mobile scan channel** **Example:** `Device# show wgb mobile scan channel`	(Optional) Displays the mobile station channels scan configuration.
Step 20	**show configuration** **Example:** `Device# show configuration`	(Optional) Displays the configuration that is stored in the NV memory.
Step 21	**show running-config** **Example:** `Device# show running-config`	(Optional) Displays the running configuration in the device.

Configuring Workgroup Bridge Timeouts (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure wgb association response timeout** *response-millisecs* **Example:** `Device# configure wgb association response timeout 4000`	Configures the WGB association response timeout. The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.
Step 2	**configure wgb authentication response timeout** *response-millisecs* **Example:** `Device# configure wgb authentication response timeout 4000`	Configures the WGB authentication response timeout. The default value is 5000 milliseconds. The valid range is between 300 and 5000 milliseconds.
Step 3	**configure wgb uclient timeout** *timeout-secs* **Example:** `Device# configure wgb uclient timeout 70`	Configure the Universal WGB client response timeout. The default timeout value is 60 seconds. The valid range is between 1 and 65535 seconds..

	Command or Action	Purpose
Step 4	**configure wgb eap timeout** *timeout-secs* **Example:** `Device# configure wgb eap timeout 20`	Configures the WGB EAP timeout. The default timeout value is 3 seconds. The valid range is between 2 and 60 seconds.
Step 5	**configure wgb channel scan timeout** {**fast**| **medium** | **slow**} **Example:** `Device# configure wgb channel scan timeout slow`	Configures the WGB channel scan timeout.
Step 6	**configure wgb dhcp response timeout** *timeout-secs* **Example:** `Device# configure wgb dhcp response timeout 70`	Configures the WGB DHCP response timeout. The default value is 60 seconds. The valid range is between 1000 and 60000 milliseconds.
Step 7	**show wgb dot11 association** **Example:** `Device# show wgb dot11 association`	Displays the WGB association summary.

Configuring Bridge Forwarding for Workgroup Bridge (CLI)

Before you begin

The Cisco Wave 2 and 11AX APs as Workgroup Bridge recognizes the Ethernet clients only when the traffic has the bridging tag.

We recommend setting the WGB bridge client timeout value to default value of 300 seconds, or less in environment where change is expected, such as:

- Ethernet cable is unplugged and plugged back.
- Endpoint is changed.
- Endpoint IP is changed (static to DHCP and vice versa).

If you need to retain the client entry in the WGB table for a longer duration, we recommend you increase the client WGB bridge timeout duration.

Procedure

	Command or Action	Purpose
Step 1	**configure wgb bridge client add** *mac-address* **Example:** `Device# configure wgb bridge client add F866.F267.7DFB-`	Adds a WGB client using the MAC address.

	Command or Action	Purpose
Step 2	**configure wgb bridge client timeout** *timeout-secs* **Example:** `Device# configure wgb bridge client timeout 400`	Configures the WGB bridge client timeout. Default timeout value is 300 seconds. The valid range is between 10 and 1000000 seconds.
Step 3	**show wgb bridge** **Example:** `Device# show wgb bridge`	Displays the WGB wired clients over the bridge.
Step 4	**show wgb bridge wired gigabitEthernet** *interface* **Example:** `Device# show wgb bridge wired gigabitEthernet 0/1`	Displays the WGB Gigabit wired clients over the bridge.
Step 5	**show wgb bridge dot11Radio** *interface-number* **Example:** `Device# show wgb bridge dot11Radio 0/3/1`	Displays the WGB bridge radio interface summary.

Information About Simplifying WGB Configuration

From Cisco IOS XE Cupertino 17.8.1, it is possible to configure WGB in multiple Cisco access points (APs) simultaneously. By importing a running configuration, you can deploy multiple WGBs in a network and make them operational quicker. When new Cisco APs are added to the network, you can transfer an existing or working configuration to the new Cisco APs to make them operational. This enhancement eliminates the need to configure multiple Cisco APs using CLIs, after logging into them.

A network administrator can onboard Cisco APs using either of the following methods:

- Upload the working configuration from an existing Cisco AP to a server and download it to the newly deployed Cisco APs.
- Send a sample configuration to all the Cisco APs in the deployment.

This feature is supported only on the following Cisco APs:

- Cisco Aironet 1562 Access Points
- Cisco Aironet 2800 Access Points
- Cisco Aironet 3800 Access Points
- Cisco Catalyst 9105 Access Points
- Cisco Catalyst 9115 Access Points
- Cisco Catalyst 9120 Access Points

- Cisco Catalyst IW6300 Series Heavy Duty Access Points

For latest support information on various features in Cisco Wave 2 and 802.11ax (Wi-Fi 6) Access Points in Cisco IOS XE releases, see the Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points document.

Configuring Multiple WGBs (CLI)

Perform the following procedure on the APs in WGB mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**copy configuration upload**{**sftp:**| **tftp:**} *ip-address* [*directory*] [*file-name*] **Example:** `Device# copy configuration upload sftp: 10.10.10.1 C:sample.txt`	Creates upload configuration file and uploads to the SFTP or TFTP server using the specified path.
Step 3	**copy configuration download**{**sftp:**| **tftp:**} *ip-address* [*directory*] [*file-name*] **Example:** `Device# copy configuration download sftp: 10.10.10.1 C:sample.txt`	Downloads the configuration file and replaces the old configuration in the AP and reboots the WGB. When the device restarts, new configuration is applied.
Step 4	**show wgb dot11 association** **Example:** `Device# show wgb dot11 association`	Lists the WGB uplink information.
Step 5	**show version** **Example:** `Device# show version`	Displays the AP software information.

Verifying WGB Configuration

After completing the configuration download and reboot of the AP, the WGB rejoins the network. Use the **show logging** command to list and verify the download events that are captured in the debug logs:

```
Device# show logging

Jan 13 18:19:17 kernel: [*01/13/2022 18:19:17.4880] WGB - Applying download config...
Jan 13 18:19:18 download_config: configure clock timezone UTC
Jan 13 18:19:18 download_config: configure dot1x credential dot1x_profile username wifiuser
 password U2FsdGVkX1+8PWmAOnFO8BXyk5EAphMy2PmhPPhWV0w=
```

```
Jan 13 18:19:18 download_config: configure eap-profile eap_profile method PEAP
Jan 13 18:19:18 download_config: configure eap-profile eap_profile dot1x-credential
dot1x_profile
Jan 13 18:19:18 chpasswd: password for user changed
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7260] chpasswd: password for user changed
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7610]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7610]  Management user configuration saved
successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7610]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7650] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7650]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7650]  Dot1x credential configuration has
been saved successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7650]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7740] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7740]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7740]  EAP profile configuration has been
saved successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7740]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7790] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7790]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7790]  EAP profile configuration has been
saved successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7790]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7830] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7830]
Jan 13 18:19:18 download_config: configure ssid-profile psk ssid alpha_psk authentication
psk U2FsdGVkX18meBfFFeiC4sgkEmbGPNH/ul1dne6h/m8= key-management wpa2
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7930] Warning!!! Attach SSID profile with the
 radio to use the new changes.
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7930]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7930]  EAP profile configuration has been
saved successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.7930]
Jan 13 18:19:18 download_config: configure ssid-profile open ssid alpha_open authentication
 open
Jan 13 18:19:18 download_config: configure ssid-profile openax ssid alpha_open_ax
authentication open
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.8650]  SSID-Profile dot1xpeap has been saved
 successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.8650]
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.9270]  SSID-Profile psk has been saved
successfully
Jan 13 18:19:18 kernel: [*01/13/2022 18:19:18.9270]
Jan 13 18:19:19 kernel: [*01/13/2022 18:19:19.0380]  SSID-Profile open has been saved
successfully
Jan 13 18:19:19 kernel: [*01/13/2022 18:19:19.0380]
Jan 13 18:19:19 kernel: [*01/13/2022 18:19:19.0380]  SSID-Profile openax has been saved
successfully
Jan 13 18:19:19 kernel: [*01/13/2022 18:19:19.0380]
Jan 13 18:19:22 download_config: configure wgb broadcast tagging disable
Jan 13 18:19:22 download_config: configure wgb packet retries 64 drop
Jan 13 18:19:22 kernel: [*01/13/2022 18:19:22.9710] Broadcast tagging 0 successfully
Jan 13 18:19:22 kernel: [*01/13/2022 18:19:22.9710]
Jan 13 18:19:23 download_config: configure dot11Radio 1 mode wgb ssid-profile open
Jan 13 18:19:23 download_config: configure dot11Radio 1 enable
Jan 13 18:19:23 download_config: configure ap address ipv6 disable
```

CHAPTER 179

Peer-to-Peer Client Support

- Information About Peer-to-Peer Client Support, on page 1987
- Configure Peer-to-Peer Client Support, on page 1987

Information About Peer-to-Peer Client Support

Peer-to-peer client support can be applied to individual WLANs, with each client inheriting the peer-to-peer blocking setting of the WLAN to which it is associated. The peer-to-Peer Client Support feature provides a granular control over how traffic is directed. For example, you can choose to have traffic bridged locally within a device, dropped by a device, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.

Restrictions

- Peer-to-peer blocking does not apply to multicast traffic.
- Peer-to-peer blocking is not enabled by default.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- FlexConnect central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect local switching. This is treated as peer-to-peer drop and client packets are dropped.

  FlexConnect central switching clients supports peer-to-peer blocking for clients associated with different APs. However, for FlexConnect local switching, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.

Configure Peer-to-Peer Client Support

Follow the procedure given below to configure Peer-to-Peer Client Support:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan wlan1`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**peer-blocking** [**allow-private-group** | **drop** | **forward-upstream**] **Example:** `Device(config-wlan)# peer-blocking drop`	Configures peer to peer blocking parameters. The keywords are as follows: • **allow-private-group**—Enables peer-to-peer blocking on the Allow Private Group action. • **drop**—Enables peer-to-peer blocking on the drop action. • **forward-upstream**—No action is taken and forwards packets to the upstream. **Note** The **forward-upstream** option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show wlan id** *wlan-id* **Example:** `Device# show wlan id 12`	Displays the details of the selected WLAN.

CHAPTER 180

Deny Wireless Client Session Establishment Using Calendar Profiles

- Information About Denial of Wireless Client Session Establishment, on page 1989
- Configuring Daily Calendar Profile, on page 1990
- Configuring Weekly Calendar Profile, on page 1991
- Configuring Monthly Calendar Profile, on page 1992
- Mapping a Daily Calendar Profile to a Policy Profile, on page 1993
- Mapping a Weekly Calendar Profile to a Policy Profile, on page 1994
- Mapping a Monthly Calendar Profile to a Policy Profile, on page 1995
- Verifying Calendar Profile Configuration, on page 1996
- Verifying Policy Profile Configuration, on page 1996

Information About Denial of Wireless Client Session Establishment

Denial of client session establishment feature allows the controller to stop client session establishment based on a particular time. This helps control the network in efficient and controlled manner without any manual intervention.

In Cisco Catalyst 9800 Series Wireless Controller , you can deny the wireless client session based on the following recurrences:

- Daily
- Weekly
- Monthly

The Calendar Profiles created are then mapped to the policy profile. By attaching the calendar profile to a policy profile, you will be able to create different recurrences for the policy profile using different policy tag.

Note You need to create separate Calendar Profile for Daily, Weekly, and Monthly sub-categories.

The following is the workflow for denial of wireless client session establishment feature:

- Create a calendar profile.
- Apply the calendar profile to a policy profile.

Note A maximum of 100 calendar profile configuration and 5 calendar profile association to policy profile is supported.

Points to Remember

If you boot up your controller, the denial of client session establishment feature kicks in after a minute from the system boot up.

If you change the system time after the calendar profile is associated to a policy profile, you can expect a maximum of 30 second delay to adapt to the new clock timings.

Note You cannot use the **no action deny-client** command to disable action while associating the calendar profile to a policy profile.

If you want to disable the action command, you need to disassociate the calendar profile from the policy profile, and re-configure again.

Configuring Daily Calendar Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile calendar-profile name** *name* **Example:** `Device(config)# wireless profile calendar-profile name daily_calendar_profile`	Configures a calendar profile. Here, *name* refers to the name of the calendar profile.
Step 3	**start** *start_time* **end** *end_time* **Example:**	Configures start and end time for the calendar profile.

	Command or Action	Purpose
	`Device(config-calendar-profile)# start 09:00:00 end 17:00:00`	Here, *start_time* is the start time for the calendar profile. You need to enter start time in **HH:MM:SS** format. *end_time* is the end time for the calendar profile. You need to enter end time in **HH:MM:SS** format.
Step 4	**recurrence daily** **Example:** `Device(config-calendar-profile)# recurrence daily`	Configures daily recurrences for a calendar profile.
Step 5	**end** **Example:** `Device(config-calendar-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. **Note** When the calendar profile kicks in, the AP power profile rules (for example, radio state and USB device state) that are defined for the Ethernet speed are not applied and continue to be as per the fixed power profile.

Configuring Weekly Calendar Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile calendar-profile name** *name* **Example:** `Device(config)# wireless profile calendar-profile name weekly_calendar_profile`	Configures a calendar profile. Here, *name* refers to the name of the calendar profile.
Step 3	**start** *start_time* **end** *end_time* **Example:** `Device(config-calendar-profile)# start 18:00:00 end 19:00:00`	Configures start and end time for the calendar profile. Here,

	Command or Action	Purpose
		start_time is the start time for the calendar profile. You need to enter start time in **HH:MM:SS** format. *end_time* is the end time for the calendar profile. You need to enter end time in **HH:MM:SS** format.
Step 4	**recurrence weekly** **Example:** `Device(config-calendar-profile)# recurrence weekly`	Configures weekly recurrences for the calendar profile.

Step 5	**day** {**friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday**}
	Example:
	`Device(config-calendar-profile)# day friday`
	`Device(config-calendar-profile)# day monday`
		Configure days when the weekly calendar needs to be active.
		Note You can configure multiple days using this command.

Step 6	**end** **Example:** `Device(config-calendar-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Monthly Calendar Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile calendar-profile name** *name* **Example:** `Device(config)# wireless profile calendar-profile name monthly_calendar_profile`	Configures a calendar profile. Here, *name* refers to the name of the calendar profile.
Step 3	**start** *start_time* **end** *end_time* **Example:** `Device(config-calendar-profile)# start 18:00:00 end 19:00:00`	Configures start and end time for the calendar profile. Here,

	Command or Action	Purpose
		start_time is the start time for the calendar profile. You need to enter start time in **HH:MM:SS** format. *end_time* is the end time for the calendar profile. You need to enter end time in **HH:MM:SS** format.
Step 4	**recurrence monthly** **Example:** `Device(config-calendar-profile)# recurrence monthly`	Configures monthly recurrences for the calendar profile.
Step 5	**date** *value* **Example:** `Device(config-calendar-profile)# date 25`	Configures a date for the calendar profile. **Note** If the requirement is to perform denial of service in certain timing, such as, 2,10, and 25 of every month, all three days need to be configured using the **date** command. There is no range for date. You need to configure the dates as per your requirement.
Step 6	**end** **Example:** `Device(config-calendar-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Mapping a Daily Calendar Profile to a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**calender-profile name** *calendar-profile-name* **Example:**	Maps a calendar profile to a policy profile. The *calendar-profile-name* is the name of the calendar profile name created in #unique_2501.

	Command or Action	Purpose
	`Device(config-wireless-policy)# calender-profile name daily_calendar_profile`	**Note** You need to disable Policy Profile before associating a calendar profile to a policy profile. The following needs to be done: `Device(config-wireless-policy)# shutdown`
Step 4	**action deny-client** **Example:** `Device(config-policy-profile-calender)# action deny-client`	Configures deny client session establishment during calendar profile interval. **Note** Client associations are denied daily between timeslot 9:00:00 to 17:00:00. For start and end time details, see #unique_2501.
Step 5	**end** **Example:** `Device(config-policy-profile-calender)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Mapping a Weekly Calendar Profile to a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**calender-profile name** *calendar-profile-name* **Example:** `Device(config-wireless-policy)# calender-profile name weekly_calendar_profile`	Maps a calender profile to a policy profile. The *calendar-profile-name* is the name of the calendar profile name created in #unique_2503. **Note** You need to disable Policy Profile before associating a calendar profile to a policy profile. The following needs to be done: `Device(config-wireless-policy)# shutdown`

	Command or Action	Purpose
Step 4	**action deny-client** **Example:** `Device(config-policy-profile-calender)# action deny-client`	Configures deny client session establishment during calendar profile interval. **Note** Client associations are denied daily between timeslot 9:00:00 to 17:00:00. For start and end time details, see #unique_2503. On Monday and Tuesday, clients are denied between 17:30:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00. On 25th of every month, clients are denied between 18:00:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.
Step 5	**end** **Example:** `Device(config-policy-profile-calender)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Mapping a Monthly Calendar Profile to a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Creates policy profile for the WLAN. The *profile-name* is the profile name of the policy profile.
Step 3	**calender-profile name** *calendar-profile-name* **Example:** `Device(config-wireless-policy)# calender-profile name monthly_calendar_profile`	Maps a calender profile to a policy profile. The *calendar-profile-name* is the name of the calendar profile name created in #unique_2505.
Step 4	**action deny-client** **Example:**	Configures deny client session establishment for the defined calendar profile interval.

	Command or Action	Purpose
	`Device(config-policy-profile-calender)# action deny-client`	**Note** Every day client associations are denied between timeslot 9:00:00 to 17:00:00. For start and end time details, see #unique_2505. On Monday and Tuesday, clients are denied between 17:30:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00. On 25th of every month, clients are denied between 18:00:00 and 19:00:00 besides regular time 9:00:00 to 17:00:00.
Step 5	**end** **Example:** `Device(config-policy-profile-calender)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Calendar Profile Configuration

To view the summary of calendar profiles, use the following command:

```
Device# show wireless profile calendar-profile summary
Number of Calendar Profiles: 3

Profile-Name
---------------------------------
monthly_25_profile
weekly_mon_profile
daily_calendar_profile
```

To view the calendar profile details for a specific profile name, use the following command:

```
Device# show wireless profile calendar-profile detailed daily_calendar_profile
Calendar profiles                          : daily_calendar_profile
-------------------------------------------------------------------
Recurrence                                 : DAILY
Start Time                                 : 09:00:00
End Time                                   : 17:00:00
```

Verifying Policy Profile Configuration

To view the detailed parameters for a specific policy profile, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile
Tunnel Profile
  Profile Name                      : Not Configured
Calendar Profile
  Profile Name                      : monthly_25_profile
  Wlan Enable                       : Not Configured
```

```
  Client Block                      : Client Block Configured
  ----------------------------------------------------
  Profile Name                      : weekly_mon_profile
  Wlan Enable                       : Not Configured
  Client Block                      : Client Block Configured
  ----------------------------------------------------
  Profile Name                      : daily_calendar_profile
  Wlan Enable                       : Not Configured
  Client Block                      : Client Block Configured
  ----------------------------------------------------
Fabric Profile
  Profile Name                      : Not Configured
```

To view the configured calendar profile information under policy profile, use the following command:

```
Device# show wireless profile policy all
Tunnel Profile
Profile Name : Not Configured
Calendar Profile
Profile Name : daily_calendar_profile
Wlan Enable : Not Configured
Client Block : Client Block Configured
----------------------------------------------------
Profile Name : weekly_calendar_profile
Wlan Enable : Not Configured
Client Block : Client Block Configured
----------------------------------------------------
Fabric Profile
Profile Name : Not Configured
```

Note The anchor priority is always displayed as local. Priorities can be assigned on the foreign controller.

CHAPTER 181

Ethernet over GRE

- Introduction to EoGRE, on page 1999
- Create a Tunnel Gateway, on page 2001
- Configuring the Tunnel Gateway (GUI), on page 2002
- Configuring a Tunnel Domain, on page 2002
- Configuring Tunnel Domain (GUI), on page 2003
- Configuring EoGRE Global Parameters, on page 2004
- Configuring EoGRE Global Parameters (GUI), on page 2004
- Configuring a Tunnel Profile, on page 2005
- Configuring the Tunnel Profile (GUI), on page 2006
- Associating WLAN to a Wireless Policy Profile, on page 2007
- Attaching a Policy Tag and a Site Tag to an AP, on page 2008
- Verifying the EoGRE Tunnel Configuration, on page 2008

Introduction to EoGRE

Ethernet over GRE (EoGRE) is an aggregation solution for grouping Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end-host, and encapsulate the traffic in Ethernet packets over an IP Generic Routing Encapsulation (GRE) tunnel. When the IP GRE tunnels are terminated on a service provider's broadband network gateway, the end-host traffic is forwarded and subscriber sessions are initiated.

Client IPv6

Client IPv6 traffic is supported on IPv4 EoGRE tunnels. A maximum of eight different client IPv6 addresses are supported per client. Wireless controller s send all the client IPv6 addresses that they have learned to the accounting server using the accounting update message. All RADIUS or accounting messages exchanged between controller s and tunnel gateways or RADIUS servers are outside the EoGRE tunnel.

EoGRE for WLAN

To enable EoGRE for a WLAN, the wireless policy profile should be mapped to a tunnel profile, which may contain the following:

- AAA override: Allows you to bypass rule filtering for a client.
- Gateway RADIUS proxy: Allows forwarding of AAA requests to tunnel gateways.

- Tunnel rules: Defines the domain to use for each realm. They also define VLAN tagging for the client traffic towards tunnel gateways.
- DHCP option 82: Provides a set of predefined fields.

EoGRE Deployment with Multiple Tunnel Gateways

The wireless controller embedded wireless controller sends keepalive pings to the primary and secondary tunnel gateways and keeps track of the missed pings. When a certain threshold level is reached for the missed pings, switchover is performed and the secondary tunnel is marked as active. This switchover deauthenticates all the clients to enable them to rejoin the access points (APs). When the primary tunnel come back online, all the client traffic are reverted to the primary tunnel. However, this behavior depends on the type of redundancy.

Load Balancing in EtherChannels

Load balancing of tunneled traffic over Etherchannels works by hashing the source or destination IP addresses or mac addresses of the tunnel endpoint pair. Because the number of tunnels is very limited when compared to clients (each tunnel carries traffic for many clients), the spreading effect of hashing is highly reduced and optimal utilization of Etherchannel links can be hard to achieve.

Using the EoGRE configuration model, you can use the *tunnel source* option of each tunnel interface to adjust the load-balancing parameters and spread tunnels across multiple links.

You can use different source interfaces on each tunnel for load balancing based on the source or destination IP address. For that choose the source interface IP address in such a way that traffic flows take different links for each src-dest IP pair. The following is an example with four ports:

```
Client traffic on Tunnel1 – Src IP: 40.143.0.72  Dest IP: 40.253.0.2
Client traffic on Tunnel2 – Src IP: 40.146.0.94  Dest IP: 40.253.0.6
Client traffic on Tunnel3 – Src IP: 40.147.0.74  Dest IP: 40.253.0.10
```

Use the **show platform software port-channel link-select interface port-channel 4 ipv4** *src_ip dest_ip* command to determine the link that a particular flow will take.

EoGRE Configuration Overview

The EoGRE solution can be deployed in two different ways:

- Central-Switching: EoGRE tunnels connect the controller to the tunnel gateways.
- Flex or Local-Switching: EoGRE tunnels are initiated on the APs and terminated on the tunnel gateways.

To configure EoGRE, perform the following tasks:

1. Create a set of tunnel gateways.
2. Create a set of tunnel domains.
3. Create a tunnel profile with rules that define how to match clients to domains.
4. Create a policy profile and attach the tunnel profile to it.
5. Map the policy profile to WLANs using policy tags.

Note The EoGRE tunnel fallback to the secondary tunnel is triggered after the *max-skip-count* ping fails in the last measurement window. Based on the starting and ending instance of the measurement window, the fall-back may take more time than the duration that is configured.

Table 141: EoGRE Authentication Methods

Method Name	First Supported Release	Mode
PSK	17.2.1	Local/Flex (central authentication)
Open	16.12.1	Local/Flex (central authentication)
LWA	16.12.1	Local/Flex (central authentication)
Dot1x	16.12.1	Local/Flex (central authentication)
CWA	16.12.1	Local/Flex (central authentication)

Create a Tunnel Gateway

Note In the Cisco Catalyst 9800 Series Wireless Controller , a tunnel gateway is modeled as a tunnel interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface tunnel** *tunnel_number* **Example:** `Device(config)# interface tunnel 21`	Configures a tunnel interface and enters interface configuration mode.
Step 3	**tunnel source** *source_intf* **Example:** `Device(config-if)# tunnel source 22`	Sets the source address of the tunnel interface. The source interface can be VLAN, Gigabit Ethernet or loopback.
Step 4	**tunnel destination** *tunnel-address* **Example:** `Device(config-if)# tunnel destination 10.11.12.13`	Sets the destination address of the tunnel.

	Command or Action	Purpose
Step 5	**tunnel mode ethernet gre** {**ipv4** | **ipv6**} **p2p** **Example:** `Device(config-if)# tunnel mode ethernet gre ipv4 p2p`	Sets the encapsulation mode of the tunnel to Ethernet over GRE IPv4 or Ethernet over GRE IPv6.

Configuring the Tunnel Gateway (GUI)

Follow the steps given below to configure the tunnel gateway:

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **EoGRE**.

Step 2 Click the **Gateways** tab.
The **Add Gateway** window is displayed.

Step 3 In the **Tunnel Id** field, specify the tunnel ID.

Step 4 In the **Destination address(IPv4/IPv6)** field, specify the IPv4 or IPv6 address.

Step 5 From the **Source Interface** drop-down list, select an interface.

Step 6 In the **AAA Proxy** section, slide the **AAA Proxy** slider to **Enabled**. When AA Proxy is enabled, complete the following steps:

a) From the **Encryption Type** drop-down list, select either **UNENCRYPTED** or **AES ENCRYPTION**.
b) In the **Key Phrase** field, specify the key phrase.

Step 7 Click **Apply to Device**.

Configuring a Tunnel Domain

Note Tunnel domains are a redundancy grouping of tunnels. The following configuration procedure specifies a primary and a secondary tunnel, along with a redundancy model.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**tunnel eogre domain** *domain* **Example:** `Device(config)# tunnel eogre domain dom1`	Configures EoGRE redundancy domain.
Step 3	**primary tunnel** *primary-tunnel_intf* **Example:** `Device(config-eogre-domain)# primary tunnel 21`	Configures the primary tunnel.
Step 4	**secondary tunnel** *secondary-tunnel_intf* **Example:** `Device(config-eogre-domain)# secondary tunnel 22`	Configures the secondary tunnel.
Step 5	**redundancy revertive** **Example:** `Device(config-eogre-domain)# redundancy revertive`	Sets the redundancy model as revertive. When redundancy is set to revertive and the primary tunnel goes down, a switchover to secondary tunnel is performed. When the primary tunnel comes back up, a switchover to the primary tunnel is performed, because the primary tunnel has priority over the secondary tunnel. When redundancy is not set to revertive, tunnels will have the same priority, and a switchover to the primary tunnel is not performed if the active tunnel is the secondary tunnel and the primary tunnel comes back up.

Configuring Tunnel Domain (GUI)

Follow the steps given below to configure the tunnel domain:

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **EoGRE**.

Step 2 Click the **Domains** tab.
The **Add Domain** window is displayed.

Step 3 In the **Name** field, specify the domain name. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 From the **Primary Tunnel Gateway** drop-down list, choose an option.

Step 5 From the **Secondary Tunnel Gateway** drop-down list, choose an option.

Step 6 Slide the **Status** button to **Enabled**, to activate the domain status.

Step 7 Slide the **Revertive Redundancy** button to **Enabled**, to activate revertive redundancy.

Step 8 Click **Apply to Device**.

Configuring EoGRE Global Parameters

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**tunnel eogre heartbeat interval** *interval-value* **Example:** `Device(config)# tunnel eogre heartbeat interval 600`	Sets EoGRE tunnel heartbeat periodic interval.
Step 3	**tunnel eogre heartbeat max-skip-count** *skip-count* **Example:** `Device(config)# tunnel eogre heartbeat max-skip-count 7`	Sets the maximum number of tolerable dropped heartbeats. After reaching the maximum number of heartbeats that can be dropped, the tunnel is declared as down and a switchover is performed.
Step 4	**tunnel eogre source loopback** *tunnel_source* **Example:** `Device(config)# tunnel eogre source loopback 12`	Sets the tunnel EoGRE source interface.
Step 5	**tunnel eogre interface tunnel** *tunnel-intf* **aaa proxy key** *key key-name* **Example:** `Device(config)# tunnel eogre interface tunnel 21 aaa proxy key 0 mykey`	(Optional) Configures AAA proxy RADIUS key for the AAA proxy setup. **Note** When the tunnel gateway is behaving as the AAA proxy server, only this step is required for the configuration.

Configuring EoGRE Global Parameters (GUI)

Follow the steps given below to configure the EoGRE global parameters:

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **EoGRE**.

The EoGRE **Global Config** tab is displayed.

Step 2 In the **Heartbeat Interval (seconds)** field, specify an appropriate timer value for heartbeat interval. The valid range is between 60 and 600 seconds.

Step 3 In the **Max Heartbeat Skip Count** field, specify the maximum heartbeat skip count. The valid range is between 3 and 10.

Step 4 From the **Interface Name** drop-down list, choose an interface name.

Step 5 Click **Apply**.

Configuring a Tunnel Profile

Before you begin

Ensure that you define the destination VLAN on the controller. If you do not define the VLAN, clients will not be able to connect.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy eogre_policy`	Configures a WLAN policy profile.
Step 3	**tunnel-profile** *tunnel-profile-name* **Example:** `Device(config-wireless-policy)# tunnel-profile tunnel1`	Creates a tunnel profile.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.
Step 5	**wireless profile tunnel** *tunnel-profile-name* **Example:** `Device(config)# wireless profile tunnel wl-tunnel-1`	Configures a wireless tunnel profile.
Step 6	**dhcp-opt82 enable** **Example:**	Activates DHCP Option 82 for the tunneled clients.

	Command or Action	Purpose
	`Device(config-tunnel-profile)# dhcp-opt82 enable`	
Step 7	**dhcp-opt82 remote-id** *remote-id* **Example:** `Device(config-tunnel-profile)# dhcp-opt82 remote-id vlan`	Configures Remote ID options. Choose from the comma-separated list of options such as **ap-mac**, **ap-ethmac**, **ap-name**, **ap-group-name**, **flex-group-name**, **ap-location**, **vlan**, **ssid-name**, **ssid-type**, and **client-mac**.
Step 8	**aaa-override** **Example:** `Device(config-tunnel-profile)# aaa-override`	Enables AAA policy override.
Step 9	**gateway-radius-proxy** **Example:** `Device(config-tunnel-profile)# gateway-radius-proxy`	Enables the gateway RADIUS proxy.
Step 10	**gateway-accounting-radius-proxy** **Example:** `Device(config-tunnel-profile)# gateway-accounting-radius-proxy`	Enables the gateway accounting RADIUS proxy.
Step 11	**rule** *priority* **realm-filter** *realm* **domain** *domain-name* **vlan** *vlan-id* **Example:** `Device(config-tunnel-profile)# rule 12 realm-filter realm domain dom1 vlan 5`	Creates a rule to choose a domain, using the realm filter, for client Network Access Identifier (NAI), tunneling domain name, and destination VLAN.

Configuring the Tunnel Profile (GUI)

Follow the steps given below to configure the tunnel profile:

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **EoGRE**.

Step 2 Click the **Tunnel Profiles** tab.

Step 3 Click the **Add** button.
The **Add Tunnel Profile** window is displayed.

Step 4 Click the **General** tab and complete the following steps:

a) In the **Name** field, specify the tunnel profile name. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

b) In the **Status** field, slide the button to change the status to **Enabled**.
c) In the **Central Forwarding** field, slide the button to **Enabled**, to enable the feature.
d) In the **DHCP Option-82** section, change the **Status** field and the **ASCII** field to **Enabled**, as per requirement.
e) In the **Delimiter** field, specify the delimiter.
f) From the **Circuit ID Available Services** list, select an available services and click the > sign to add the services to the assigned list.
g) From the **Remote ID Available Services** list, select an available services and click the > sign to add the services to the assigned list.
h) In the **AAA** section, choose an appropriate status for the **Radius Proxy** field, the **Accounting Proxy** field, and the **Override** field.

Step 5 Click the **Rules** tab, and complete the following steps:

a) Click the **Add Rules** button.
b) In the **Priority** field, specify the priority of the rule from a range of 1 to 100.
c) In the **Realm** field, specify a realm.
d) From the **Domain** drop-down list, choose a domain.
e) In the **VLAN Id** field, specify the VLAN ID that ranges between 1 and 4094.
f) Click **Save**.

Step 6 Click **Apply to Device**.

Associating WLAN to a Wireless Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy eogre_tag`	Configures a policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan eogre_open_eogre policy eogre_policy`	Maps an EoGRE policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.

Attaching a Policy Tag and a Site Tag to an AP

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap 80E8.6FD4.0BB0`	Configures an AP and enters AP profile configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag eogre_tag`	Maps the EoGRE policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag sp-flex-site`	Maps a site tag to the AP.
Step 5	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.

Verifying the EoGRE Tunnel Configuration

The `show tunnel eogre` command displays the EoGRE clients, domains, gateways, global-configuration, and manager information in the local mode.

To display the EoGRE domain summary in the local mode, use the following command:

```
Device# show tunnel eogre domain summary

Domain Name          Primary GW   Secondary GW      Active GW      Redundancy
-------------------------------------------------------------------------------
domain1              Tunnel1      Tunnel2           Tunnel1        Non-Revertive
eogre_domain         Tunnel1      Tunnel2           Tunnel1        Non-Revertive
```

To display the details of an EoGRE domain in the local mode, use the following command:

```
Device# show tunnel eogre domain detailed domain-name

Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
```

```
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
```

To view the EoGRE tunnel gateway summary and statistics in the local mode, use the following command:

```
Device# show tunnel eogre gateway summary

Name               Type  Address                                  AdminState  State  Clients
-------------------------------------------------------------------------------------------
Tunnel1             IPv4  9.51.1.11                                 Up          Up     0

Tunnel2             IPv4  9.51.1.12                                 Up          Down   0

Tunnel10            IPv6  fd09:9:8:21::90                           Down        Down   0

Tunnel11            IPv4  9.51.1.11                                 Up          Up     0

Tunnel12            IPv6  fd09:9:8:21::90                           Up          Down   0

Tunnel100           IPv4  9.51.1.100                                Up          Down   0
```

To view the details of an EoGRE tunnel gateway in the local mode, use the following command:

```
Device# show tunnel eogre gateway detailed gateway-name

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 Source : Vlan51 / 9.51.1.1
 State  : Up
 SLA ID : 56
 MTU    : 1480
 Up Time: 4 minutes 45 seconds

 Clients
  Total Number of Wireless Clients      : 0
 Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
  Total Number of Transmitted Bytes     : 0
 Keepalives
  Total Number of Lost Keepalives       : 0
  Total Number of Received Keepalives   : 5
  Total Number of Transmitted Keepalives: 5
  Windows                               : 1
  Transmitted Keepalives in last window : 2
  Received Keepalives in last window    : 2
```

To view the client summary of EoGRE in the local mode, use the following command:

```
Device# show tunnel eogre client summary

Client MAC      AP MAC          Domain                          Tunnel        VLAN  Local
-------------------------------------------------------------------------------------------
74da.3828.88b0  80e8.6fd4.9520  eogre_domain                     N/A           2121   No
```

To view the details of an EoGRE global configuration in the local mode, use the following command:

```
Device# show tunnel eogre global-configuration
```

```
Heartbeat interval       : 60
Max Heartbeat skip count : 3
Source Interface         : (none)
```

To view the details of the global tunnel manager statistics in the local mode, use the following command:

```
Device# show tunnel eogre manager stats global

Tunnel Global Statistics
Last Updated                     : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                       : 6
  Domains                        : 2

EoGRE Flex Objects
  AP Gateways                    : 2
  AP Domains                     : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates             : 806
  IOS Domain updates             : 88
  Global updates                 : 48
  Tunnel Profile updates         : 120
  Tunnel Rule updates            : 16
  AAA proxy key updates          : 0

AP events
  Flex AP Join                   : 1
  Flex AP Leave                  : 0
  Local AP Join                  : 0
  Local AP leave                 : 0
  Tunnel status (rx)             : 4
  Domain status (rx)             : 1
  IAPP stats msg (rx)            : 3
  Client count (rx)              : 6
  VAP Payload msg (tx)           : 4
  Domain config (tx)             : 1
  Global config (tx)             : 1
  Client delete (tx)             : 1
  Client delete per domain (tx)  : 3
  DHCP option 82 (tx)            : 4

Client events
  Add-mobile                     : 2
  Run-State                      : 3
  Delete                         : 1
  Cleanup                        : 0
  Join                           : 2
  Plumb                          : 0
  Join Errors                    : 0
  HandOff                        : 0
  MsPayload                      : 2
  FT Recover                     : 0
  Zombie GW counter increase     : 0
  Zombie GW counter decrease     : 0
  Tunnel Profile reset           : 88
  Client deauth                  : 0
  HA reconciliation              : 0

Client Join Events
  Generic Error                  : 0
  MSPayload Fail                 : 0
  Invalid VLAN                   : 0
```

```
  Invalid Domain                : 0
  No GWs in Domain              : 0
  Domain Shut                   : 0
  Invalid GWs                   : 0
  GWs Down                      : 0
  Rule Match Error              : 0
  AAA-override                  : 0
  Flex No Active GW             : 0
  Open Auth join attempt        : 2
  Dot1x join attempt            : 2
  Mobility join attempt         : 0
  Tunnel Profile not valid      : 2
  Tunnel Profile valid          : 2
  No rule match                 : 0
  Rule match                    : 2
  AAA proxy                     : 0
  AAA proxy accounting          : 0
  AAA eogre attributes          : 0
  Has aaa override              : 0
  Error in handoff payload      : 0
  Handoff AAA override          : 0
  Handoff no AAA override       : 0
  Handoff payload received      : 0
  Handoff payload sent          : 0

SNMP Traps
  Client                        : 0
  Tunnel                        : 2
  Domain                        : 0

IPC
  IOSd TX messages              : 0

Zombie Client
  Entries                       : 0
```

To view the tunnel manager statistics of a specific process instance in the local mode, use the following command:

```
Device# show tunnel eogre manager stats instance instance-number

Tunnel Manager statistics for process instance : 0
Last Updated                    : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                      : 6
  Domains                       : 2

EoGRE Flex Objects
  AP Gateways                   : 2
  AP Domains                    : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates            : 102
  IOS Domain updates            : 11
  Global updates                : 6
  Tunnel Profile updates        : 15
  Tunnel Rule updates           : 2
  AAA proxy key updates         : 0

AP events
  Flex AP Join                  : 1
```

```
  Flex AP Leave                  : 0
  Local AP Join                  : 0
  Local AP leave                 : 0
  Tunnel status (rx)             : 4
  Domain status (rx)             : 1
  IAPP stats msg (rx)            : 3
  Client count (rx)              : 6
  VAP Payload msg (tx)           : 4
  Domain config (tx)             : 1
  Global config (tx)             : 1
  Client delete (tx)             : 1
  Client delete per domain (tx)  : 3
  DHCP option 82 (tx)            : 4

Client events
  Add-mobile                     : 2
  Run-State                      : 3
  Delete                         : 1
  Cleanup                        : 0
  Join                           : 2
  Plumb                          : 0
  Join Errors                    : 0
  HandOff                        : 0
  MsPayload                      : 2
  FT Recover                     : 0
  Zombie GW counter increase     : 0
  Zombie GW counter decrease     : 0
  Tunnel Profile reset           : 11
  Client deauth                  : 0
  HA reconciliation              : 0

Client Join Events
  Generic Error                  : 0
  MSPayload Fail                 : 0
  Invalid VLAN                   : 0
  Invalid Domain                 : 0
  No GWs in Domain               : 0
  Domain Shut                    : 0
  Invalid GWs                    : 0
  GWs Down                       : 0
  Rule Match Error               : 0
  AAA-override                   : 0
  Flex No Active GW              : 0
  Open Auth join attempt         : 2
  Dot1x join attempt             : 2
  Mobility join attempt          : 0
  Tunnel Profile not valid       : 2
  Tunnel Profile valid           : 2
  No rule match                  : 0
  Rule match                     : 2
  AAA proxy                      : 0
  AAA proxy accounting           : 0
  AAA eogre attributes           : 0
  Has aaa override               : 0
  Error in handoff payload       : 0
  Handoff AAA override           : 0
  Handoff no AAA override        : 0
  Handoff payload received       : 0
  Handoff payload sent           : 0

SNMP Traps
  Client                         : 0
  Tunnel                         : 2
  Domain                         : 0
```

```
IPC
  IOSd TX messages              : 0

Zombie Client
  Entries                       : 0
```

The `show ap tunnel eogre` command displays the tunnel domain information, EoGRE events, and the tunnel gateway status on the APs, in the flex mode.

To view the summary information of an EoGRE tunnel gateway in the flex mode, use the following command:

```
Device# show ap tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-------------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain                    Tunnel1
```

To view the wireless tunnel profile summary, use the following command:

```
Device# show wireless profile tunnel summary

Profile Name                    AAA-Override AAA-Proxy DHCP Opt82 Enabled
------------------------------- ------------ --------- ---------- ---------
eogre_tunnel                             No        No        Yes       Yes
eogre_tunnel_set                         No        No        Yes        No
eogre_tunnel_snmp                        No        No         No        No
```

To view a wireless tunnel profile's details, use the following command:

```
Device# show wireless profile tunnel detailed profile-name

Profile Name : eogre_tunnel
Status : Enabled
 AAA-Proxy/Accounting-Proxy: Disabled / Disabled
 AAA-Override : Disabled
 DHCP Option82 : Enabled
  Circuit-ID : ap-mac,ap-ethmac,ap-location,vlan
  Remote-ID : ssid-name,ssid-type,client-mac,ap-name

Tunnel Rules

Priority Realm                Vlan Domain (Status/Primary GW/Secondary GW)
-------- -------------------- ---- ---------------------------------------
1        *                    2121 eogre_domain (Enabled/Tunnel1/Tunnel2)
```

To view detailed information about an EoGRE tunnel domain's status, use the following command:

```
Device# show ap tunnel eogre domain detailed

Domain     : eogre_domain
AP MAC     : 80e8.6fd4.9520
Active GW  : Tunnel1
```

To view the EoGRE events on an AP, use the following command:

```
Device# show ap tunnel eogre events

AP 80e8.6fd4.9520  Event history
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
```

```
02/18/2019 23:50:26.341 6        IAPP_STATS           0 GW Tunnel2 uptime:0s

02/18/2019 23:49:40.222 2        CLIENT_JOIN         0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:48:43.549 1        CLIENT_LEAVE        0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:47:33.127 1        DOMAIN_STATUS        0 eogre_domain Active GW: Tunnel1

02/18/2019 23:47:33.124 4        AP_TUNNEL_STATUS     0 Tunnel2 Dn

02/18/2019 23:47:33.124 1        MSG_CLIENT_DEL       0 GW Tunnel2 (IP: 9.51.1.12)

02/18/2019 23:47:33.124 2        TUNNEL_ADD           0 GW Tunnel2

02/18/2019 23:47:33.120 3        MSG_CLIENT_DEL_PD    0 GW Tunnel1 (IP: 9.51.1.11)

02/18/2019 23:47:31.763 2        AP_DOMAIN_PUSH       0 Delete:eogre_domain_set, 0 GWs

02/18/2019 23:47:31.753 4        AP_VAP_PUSH          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

To view the summary information of the EoGRE tunnel gateway, use the following command:

```
Device# show ap tunnel eogre gateway summary

AP MAC          Gateway          Type  IP                                          State  Clients
-------------------------------------------------------------------------------------------------
80e8.6fd4.9520  Tunnel1          IPv4  9.51.1.11                                     Up     1

80e8.6fd4.9520  Tunnel2          IPv4  9.51.1.12                                     Down   0
```

To view detailed information about an EoGRE tunnel gateway, use the following command:

```
Device# show ap tunnel eogre gateway detailed gateway-name

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 State  : Up
 MTU    : 1476
 Up Time: 14 hours 25 minutes 2 seconds
 AP MAC : 80e8.6fd4.9520

 Clients
  Total Number of Wireless Clients      : 1
 Traffic
  Total Number of Received Packets      : 6
  Total Number of Received Bytes        : 2643
  Total Number of Transmitted Packets   : 94
  Total Number of Transmitted Bytes     : 20629
  Total Number of Lost Keepalive        : 3
```

To view summary information about the EoGRE tunnel gateway status, use the following command:

```
Device# show ap tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-------------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain                    Tunnel1
```

To view information about EoGRE events on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre events

AP 80e8.6fd4.9520  Event history
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
---------------------------------------
02/18/2019 23:50:26.341 6        IAPP_STATS           0 GW Tunnel2 uptime:0s

02/18/2019 23:49:40.222 2        CLIENT_JOIN         0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:48:43.549 1        CLIENT_LEAVE        0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:47:33.127 1        DOMAIN_STATUS        0 eogre_domain Active GW: Tunnel1

02/18/2019 23:47:33.124 4        AP_TUNNEL_STATUS     0 Tunnel2 Dn

02/18/2019 23:47:33.124 1        MSG_CLIENT_DEL       0 GW Tunnel2 (IP: 9.51.1.12)

02/18/2019 23:47:33.124 2        TUNNEL_ADD           0 GW Tunnel2

02/18/2019 23:47:33.120 3        MSG_CLIENT_DEL_PD    0 GW Tunnel1 (IP: 9.51.1.11)

02/18/2019 23:47:31.763 2        AP_DOMAIN_PUSH       0 Delete:eogre_domain_set, 0 GWs

02/18/2019 23:47:31.753 4        AP_VAP_PUSH          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

To view the summary information about EoGRE tunnel domain's status on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-------------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain
```

To view the detailed information about EoGRE tunnel domain on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre domain detailed

Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
 AdminState    : Up
```

To view the summary information about EoGRE tunnel gateways on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre gateway summary

AP MAC          Gateway          Type  IP                                      State  Clients
-----------------------------------------------------------------------------------------------
80e8.6fd4.9520  Tunnel1          IPv4  9.51.1.11                                 Up     1

80e8.6fd4.9520  Tunnel2          IPv4  9.51.1.12                                 Down   0
```

To view detailed information about an EoGRE tunnel gateway's status on an AP, use the following command:

```
Device# show ap name ap-name tunnel eogre gateway detailed gateway-name

Gateway : Tunnel2
 Mode   : IPv4
```

```
IP     : 9.51.1.12
State  : Down
MTU    : 0
AP MAC : 80e8.6fd4.9520

Clients
 Total Number of Wireless Clients      : 0
Traffic
 Total Number of Received Packets      : 0
 Total Number of Received Bytes        : 0
 Total Number of Transmitted Packets   : 0
 Total Number of Transmitted Bytes     : 0
 Total Number of Lost Keepalive        : 151
```

CHAPTER 182

Wireless Guest Access

- Wireless Guest Access, on page 2017
- Load Balancing Among Multiple Guest Controllers, on page 2021
- Guidelines and Limitations for Wireless Guest Access, on page 2021
- Configure Mobility Tunnel for Guest Access (GUI), on page 2022
- Configure Mobility Tunnel for Guest Access (CLI), on page 2022
- Configuring Guest Access Policy (GUI), on page 2022
- Configuring Guest Access Policy (CLI), on page 2023
- Viewing Guest Access Debug Information (CLI), on page 2025
- Configure Guest Access Using Different Security Methods, on page 2025

Wireless Guest Access

The Wireless Guest Access feature addresses the need to provide internet access to guests in a secure and accountable manner. The implementation of a wireless guest network uses the enterprise's existing wireless and wired infrastructure to the maximum extent. This reduces the cost and complexity of building a physical overlay network. Wireless Guest Access solution comprises of two controllers - a Guest Foreign and a Guest Anchor. An administrator can limit bandwidth and shape the guest traffic to avoid impacting the performance of the internal network.

Note

- When a client joins through a capwap tunnel from an AP, the RADIUS NAS-Port-Type is set as "wireless 802.11". Here, Point of Attachment (PoA) and Point of Presence (PoP) is the same.
- When a client joins through a mobility tunnel, the RADIUS NAS-Port-Type is set as "virtual". Here, PoA is the Foreign controller and PoP is the Anchor controller as the client is anchored. For information on the standard types, see the following link:

  https://www.iana.org/assignments/radius-types/radius-types.xhtml#radius-types-13

Wireless Guest Access feature comprises the following functions:

- Guest Anchor controller is the point of presence for a client.
- Guest Anchor Controller provides internal security by forwarding the traffic from a guest client to a Cisco Wireless Controller in the demilitarized zone (DMZ) network through the anchor controller.

- Guest Foreign controller is the point of attachment of the client.
- Guest Foreign Controller is a dedicated guest WLAN or SSID and is implemented throughout the campus wireless network wherever guest access is required. A WLAN with mobility anchor (guest controller) configured on it identifies the guest WLAN.
- Guest traffic segregation implements Layer 2 or Layer 3 techniques across the campus network to restrict the locations where guests are allowed.
- Guest user-level QoS is used for rate limiting and shaping, although it is widely implemented to restrict the bandwidth usage for a guest user.
- Access control involves using embedded access control functionality within the campus network, or implementing an external platform to control guest access to the Internet from the enterprise network.
- Authentication and authorization of guests that are based on variables, including date, duration, and bandwidth.
- An audit mechanism to track who is currently using, or has used, the network.
- A wider coverage is provided by including areas such as lobbies and other common areas that are otherwise not wired for network connectivity.
- The need for designated guest access areas or rooms is removed.

Note To use IRCM with AireOS in your network, contact Cisco TAC for assistance.

Table 142: Supported Controllers

Controller Name	Supported as Guest Anchor	Supported as Guest Foreign
Cisco Catalyst 9800-40 Wireless Controller	Yes	Yes
Cisco Catalyst 9800-80 Wireless Controller	Yes	Yes
Cisco Catalyst 9800-CL Wireless Controller	Yes	Yes
Cisco Catalyst 9800-L Wireless Controller	Yes	Yes
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	No	No
Cisco Catalyst 9800 Embedded Wireless Controller on Cisco Catalyst 9100 Series APs	No	No

Following is a list of features supported by Cisco Guest Access:

Supported Features

- Sleeping Clients
- FQDN
- AVC (AP upstream and downstream)
- Native Profiling
- Open Authentication
- OpenDNS
- Supported Security Methods:
  - MAB Central Web Authentication (CWA)
  - Local Web Authentication (LWA)
  - LWA on MAB Failure
  - 802.1x + CWA
  - 802.1x
  - PSK
  - 802.1x + LWA
  - PSK + CWA
  - PSK + LWA
  - iPSK + CWA
  - MAB Failure + PSK
  - MAB Failure + OWE
  - MAB Failure + SAE
- SSID QoS Upstream and Downstream (Foreign)
- AP/ Client SSO
- Static IP Roaming
- Client IPv6
- Roaming across controllers
- RADIUS Accounting

Note In a guest access scenario, accounting is always performed at the foreign controller for all authentication methods.

- QoS: Client-Level Rate Limiting

- Guest Anchor Load Balancing
- Workgroup Bridges (WGB)

Note To enable the controller to support multiple VLANs from a WGB, use **wgb vlan** command.

Foreign Map Overview

Guest Access supports Foreign Map using Policy Profile and WLAN Profile configuration models in Cisco Catalyst 9800 Series Wireless Controller.

Foreign Map support in Cisco Catalyst 9800 Series Wireless Controller is achieved with the following policy profile and WLAN profile config model.

- Guest Foreign commands:
  - **Foreign1: wlanProf1 PolicyProf1**
  - **Foreign2: wlanProf2 PolicyProf2**
- Guest Anchor commands:
  - **wlanProf1, wlanProf2**
  - **PolicyProf1: Vlan100 - subnet1**
  - **PolicyProf2: Vlan200 - subnet2**

Foreign Map Roaming

Configure two different WLAN profiles on the two Guest Foreigns and seamless roaming is not allowed between them. This is expected configuration. However, seamless roaming is allowed if the same WLAN profile is configured on two Guest Foreigns, but it prevents Foreign Map feature from working.

Wireless Guest Access: Use Cases

The wireless guest access feature can be used to meet different requirements. Some of the possibilities are shared here.

Scenario One: Providing Secured Network Access During Company Merger

This feature can be configured to provide employees of **company A** who are visiting **company B** to access company A resources on company B network securely.

Scenario Two: Shared Services over Existing Setup

Using this feature, you can provide multiple services using multiple vendors piggy backing on the existing network. A company can provide services on an SSID which is anchored on the existing controller. This is while the existing service continues to serve over the same controller and network.

Load Balancing Among Multiple Guest Controllers

- You can configure export anchors to load balance large guest client volumes. For a single export foreign guest WLAN configuration, up to 72 controllers are allowed. To configure mobility guest controllers, use **mobility anchor** *ip address*.
- You can specify primary anchors with priority (1,3) and choose another anchor as backup in case of failure.
- In a multi-anchor scenario, when the primary anchor goes down, the clients get disconnected from the primary anchor and joins the secondary anchor.

Guidelines and Limitations for Wireless Guest Access

- Match the security profiles under WLAN on both Guest Foreign, and Guest Anchor.
- Match the policy profile attributes such as NAC and AAA Override on both Guest Foreign, and Guest Anchor controllers.
- On Export Anchor, the WLAN profile name and Policy profile name is chosen when a client joins at runtime and the same should match with the Guest Foreign controller.

Troubleshooting IPv6

When a guest export client cannot get a routable IPv6 address through SLAAC or cannot pass traffic when the IPv6 address is learned through DHCPv6, you can use the following workarounds:

- On IPv6 Routers: You can work around the RA multicast to unicast conversion by modifying behavior on the IPv6 gateway. Depending on the product, this may be the default behavior or may require configuration.
  - On Cisco IPv6 Routers
    - Cisco Nexus platform: Has solicited unicast RA enabled by default to help with wireless deployment.
    - Cisco IOS-XE platform: Use the following configuration command to turn on unicast RA to help with wireless deployment:

      ipv6 nd ra solicited unicast

  - On non-Cisco IPv6 Routers: If non-Cisco network devices do not support configuration command to enable solicited unicast RA then a work around does not exist.

Configure Mobility Tunnel for Guest Access (GUI)

Procedure

Step 1 Choose **Configure** > **Tags and Profiles** > **WLANs**.

Step 2 In the **Wireless Networks** area, click the relevant WLAN or RLAN and click **Mobility Anchor**.

Step 3 In the **Wireless Network Details** section, choose a device from the **Switch IP Address** drop-down list.

Step 4 Click **Apply**.

Configure Mobility Tunnel for Guest Access (CLI)

Follow the procedure given below to configure a mobility tunnel.

Procedure

	Command or Action	Purpose
Step 1	**wireless mobility group name** *group name* **Example:** `Device(config)# wireless mobility group name mtunnelgrp`	Configures a mobility group.
Step 2	**wireless mobility mac-address** *mac address* **Example:** `Device(config)# wireless mobility mac-address 0d:4c:da:3a:f2:21`	Configures a mobility MAC address.
Step 3	**wireless mobility group member mac** *mac address* **ip** *ip address* **group** *group name* **Example:** `Device(config)# wireless mobility group member mac-address df:07:a1:a7:a8:55 ip 206.223.123.2 group mtgrp`	Configures a mobility peer.

Configuring Guest Access Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** and enable the **Central Switching** toggle button.

Step 4 In the **Access Policies** tab, under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list.

Step 5 In the **Mobility** tab, under the **Mobility Anchors** settings, check the **Export Anchor** check box.

Step 6 In the **Advanced** tab, under the **WLAN Timeout** settings, enter the **Idle Timeout (sec)**.

Step 7 Click **Apply to Device**.

Configuring Guest Access Policy (CLI)

Follow the procedure given below to create and configure the guest access profile policy. Alternately, you may use the existing default policy profile after configuring the mobility anchor to that policy.

You can only configure anchors which are peers. Ensure that the IP address that is used is a mobility peer and is included in the mobility group. The system shows an invalid anchor IP address error message when any other IP address is used.

To delete the mobility group, ensure that the mobility peer which is also a mobility anchor is removed from the policy profile.

Note

- No payload is sent to Guest Foreign to display the VLAN.
- To avoid a client exclusion from occurring due to VLAN, Cisco Catalyst 9800 Series Controllers need to define VLAN along with the associated name being pushed from ISE.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan_policy_profile* **Example:** `Device(config)# wireless profile policy guest-test-policy`	Configures the policy profile and enters wireless profile configuration mode. **Note** • You can use the **default-policy-profile** to configure the profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Shuts down the policy if it exists before configuring the anchor.
Step 4	**central switching** **Example:**	(Optional) Enables central switching.

	Command or Action	Purpose
	`Device(config-wireless-policy)# central switching`	

Step 5	Choose the first option to configure the Guest Foreign or second option to configure the Guest Anchor:
	• **mobility anchor** *anchor-ip-address*
	• **mobility anchor**
	Example:
	For Guest Foreign:
	`Device(config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device(config-wireless-policy)# mobility anchor`
		Configures Guest Foreign or Guest Anchor.

Step 6	**idle-timeout** *timeout* **Example:** `Device (config-wireless-policy)# idle-timeout 1000`	(Optional) Configures duration of idle timeout, in seconds.
Step 7	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 2`	Configures VLAN name or VLAN Id. **Note** VLAN is optional for a Guest Foreign controller.
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.
Step 9	**end** **Example:** `Device(config-wireless-policy)# end`	Exits the configuration mode and returns to privileged EXEC mode.
Step 10	**show wireless profile policy summary** **Example:** `Device# show wireless profile policy summary`	(Optional) Displays the configured profiles.
Step 11	**show wireless profile policy detailed** *policy-profile-name* **Example:** `Device# show wireless profile policy detailed guest-test-policy`	(Optional) Displays detailed information of a policy profile.

Viewing Guest Access Debug Information (CLI)

- To display client level detailed information about mobility state and the anchor IP address, use the following command:.

  show wireless client mac-add *mac-address* **detail**

- To display the client mobility statistics, use the following command:

  show wireless client mac-address *mac-address* **mobility statistics**

- To display client level roam history for an active client in sub-domain, use the following command:

  show wireless client mac-address *mac-address* **mobility history**

- To display detailed parameters of a given profile policy, use the following command:

  show wireless profile policy detailed *policy-name*

- To display the global level summary for all mobility messages, use the following command:

  show wireless mobility summary

- To display the statistics for the Mobility manager, use the following command:

  show wireless stats mobility

Configure Guest Access Using Different Security Methods

The following sections provide information about the following:

Open Authentication

To configure the guest access with open authentication, follow the steps:

1. Configuring the WLAN Profile
2. #unique_2534

Note No tag is required unless AVC is enabled.

Configure a WLAN Profile for Guest Access with Open Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**. Choose the radio policy from the **Radio Policy** drop-down list. Enable or disable the **Status** and **Broadcast SSID** toggle buttons.

Step 4 Choose **Security** > **Layer2** tab. Uncheck the **WPA Policy**, **WPA2 Policy**, **AES** and **802.1x** check boxes.

Step 5 Click **Apply to Device**.

Configure a WLAN Profile For Guest Access with Open Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid-name*. **Example:** `Device(config)# wlan mywlan 34 mywlan-ssid`	Configures the WLAN and SSID.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Saves the configuration.

Configuring a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile* **Example:** `Device(config)# wireless profile policy open_it`	Configures WLAN policy profile and enters the wireless policy configuration mode.

Step 3	Choose the first option to configure a Guest Foreign or second option to configure a Guest Anchor:
	• **mobility anchor** *anchor-ip-address*
	• **mobility anchor**
	Example:
	For Guest Foreign:
	`Device (config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device (config-wireless-policy)# mobility anchor`
		Configures Guest Foreign or Guest Anchor.

Step 4	**central switching**. **Example:** `Device(config-wireless-policy)# central switching`	Enables Central switching
Step 5	**vlan** *id* **Example:** `Device(config-wireless-policy)# vlan 16`	Configures a VLAN name or VLAN ID. **Note** VLAN is optional for a Guest Foreign controller.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

Local Web Authentication

To configure LWA, follow these steps:

1. Configure a Parameter Map (CLI)

2. Configure a WLAN Profile for Guest Access with Local Web Authentication (CLI)
3. Applying Policy Profile on a WLAN
4. Configure an AAA Server for Local Web Authentication (CLI)

Configure a Parameter Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.

Step 2 Click **Add**.

Step 3 Enter the **Parameter-map name**, **Maximum HTTP connections**,**Init-State Timeout(secs)** and choose **webauth** in the **Type** drop-down list.

Step 4 Click **Apply to Device**.

Configure a Parameter Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Device(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 3	**type webauth** **Example:** `Device(config-params-parameter-map)#type webauth`	Configures the webauth type parameter.
Step 4	**timeout init-state sec** *timeout-seconds* **Example:** `Device(config-params-parameter-map)# timeout inti-state sec 3600`	Configures the WEBAUTH timeout in seconds. Valid range for the time in sec parameter is 60 to 3932100 seconds.
Step 5	**virtual-ip ipv4** *virtual_IP_address* **Example:** `Device(config-params-parameter-map)#virtual-ip ipv4 209.165.201.1`	Configures a VLAN name or VLAN ID.

Configure a WLAN Profile for Guest Access with Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click on the **WLAN** name.

Step 3 Choose **Security** > **Layer3**.

Step 4 Check the **Web Policy** check box.

Step 5 Choose a parameter map from the **Web Auth Parameter Map** drop-down list.

Step 6 Choose an authentication list from the **Authentication List** drop-down list.

Step 7 Click **Update & Apply to Device**.

Configure a WLAN Profile for Guest Access with Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-id ssid-name* **Example:** `Device# Device(config)# wlan mywlan 38 mywlan-ssid1`	Configures the WLAN and SSID.
Step 3	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables web authentication for a WLAN.
Step 4	**security web-auth parameter-map** *default* **Example:** `Device(config-wlan)# security web-auth parameter-map default`	Configure the default parameter map. **Note** When **security web-auth** is enabled, you get to map the **default authentication-list** and global **parameter-map**. This is applicable for authentication-list and parameter-map that are not explicitly mentioned.
Step 5	**security web-auth parameter-map** *global* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Configure the global parameter map.

	Command or Action	Purpose
Step 6	**security web-auth authentication-list** *LWA-AUTHENTICATION* **Example:** `Device(config-wlan)# security web-auth authentication-list LWA-AUTHENTICATION`	Sets the authentication list for IEEE 802.1x.

Configure an AAA Server for Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **AAA Advanced** > **Global Config**.

Step 2 Choose the options from the **Local Authentication**, **Authentication Method List**, **Local Authorization** and **Authorization Method List** drop-down lists.

Step 3 Enable or Disable the **Radius Server Load Balance** using toggle button.

Step 4 Check the **Interim Update** check box.

Step 5 Click **Apply**.

Configure an AAA Server for Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication login** *LWA-AUTHENTICATION* **local** **Example:** `Device(config)#aaa authentication login lwa-authentication local`	Defines the authentication method at login.
Step 3	**aaa authorization network default local if-authenticated** **Example:** `Device(config)#aaa authorization network default local if-authenticated`	Sets the authorization method to local if the user has authenticated.

Global Configuration

Follow the procedure given below for global configuration:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**username** *name* **password 0** *clear-text-password* **Example:** `Device(config)# #username base password 0 pass1`	Sets the clear text password for the user.
Step 3	**ip http server** **Example:** `Device(config)#ip http server`	Enables the HTTP server.
Step 4	**ip http authentication local** **Example:** `Device(config)#ip http authentication local`	Sets the HTTP server authentication method to local. **Note** You will get the admin access rights regardless of the user privilege, if the **ip http authentication local** is disabled and username is the same as enable password.

Central Web Authentication

To configure CWA, follow these steps:

1. Configure a WLAN Profile for Guest Access with Central Web Authentication (CLI)
2. #unique_2548
3. AAA Server Configuration (CLI)
4. #unique_2550

Configure a WLAN Profile for Guest Access with Central Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 To enable the WLAN, set **Status** as **Enabled**.

Step 5 From the **Radio Policy** drop-down list, select the radio policy.

Step 6 To enable the **Broadcast SSID**, set the status as **Enabled**.

Step 7 Choose **Security** > **Layer2** tab. Uncheck the **WPA Policy**, **WPA2 Policy**, **AES** and **802.1x** check boxes.

Step 8 Check the **MAC Filtering** check box to enable the feature. With MAC Filtering enabled, choose the Authorization list from the **Authorization List** drop-down list.

Step 9 Click **Apply to Device**.

Configure a WLAN Profile for Guest Access with Central Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-id ssid-name* **Example:** `Device# Device(config)# wlan mywlan 38 mywlan-ssid1`	Configures the WLAN and SSID.
Step 3	**mac-filtering** *remote_authorization_list_name* **Example:** `Device(config-wlan)# mac-filtering auth-list`	Enables MAB authentication for the remote RADIUS server.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.

	Command or Action	Purpose
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Saves the configuration.

AAA Server Configuration (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups** > **RADIUS** > **Server Groups**.
Step 2 Click the RADIUS server group.
Step 3 From the **MAC-Delimiter** drop-down list, choose an option.
Step 4 From the **MAC-Filtering** drop-down list, choose an option.
Step 5 Enter the **Dead-Time (mins)**.
Step 6 From the **Available Servers** on the left, move the servers you need to **Assigned Servers** on the right.
Step 7 Click **Update & Apply to Device**.
Step 8 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups** > **RADIUS** > **Servers**.
Step 9 Click the RADIUS server.
Step 10 Enter the **IPv4/IPv6 Server Address**, **Auth Port**, **Acct Port**, **Server Timeout (seconds)** and **Retry Count**.
Step 11 Check or uncheck the **PAC Key** checkbox and choose the Key Type from the **Key Type** drop-down list. Enter the **Key** and **Confirm Key**.
Step 12 Enable or disable the **Support for CoA** toggle button.
Step 13 Click **Update & Apply to Device**.

AAA Server Configuration (CLI)

Note Configure AAA server for Guest Foreign only.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa authorization network** *authorization-list* **local group** *Server-group-name* **Example:**	Sets the authorization method to local.

	Command or Action	Purpose
	`Device(config)#aaa authorization network cwa local group ise`	
Step 3	**aaa group server radius** *server-group-name* **Example:** `Device(config)#aaa group server radius ise`	Configures RADIUS server group definition. **Note** *server-group-name* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.
Step 4	**server name** *radius-server-name* **Example:** `Device(config-sg-radius)#server name ise1`	Configures the RADIUS server name.
Step 5	**subscriber mac-filtering security-mode mac** **Example:** `Device(config-sg-radius)#$mac-filtering security-mode mac`	Sets the MAC address as the password.
Step 6	**mac-delimiter colon** **Example:** `Device(config-sg-radius)#mac-delimiter colon`	Sets the MAC address delimiter to colon.
Step 7	**end** **Example:** `Device(config-sg-radius)#end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 8	**radius server** *name* **Example:** `Device(config)#radius server ISE1`	Sets the RADIUS server name
Step 9	**address ipv4** *radius-server-ipaddress* **auth-port** *port-number* **acct-port** *port-number* **Example:** `Device(config-radius-server)#address ipv4 209.165.201.1 auth-port 1635 acct-port 33`	Configures the RADIUS server IP address authentication and accounting ports.

Configuring 802.1x with Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wlan** *wlan-profile wlan-id ssid* **Example:** `Device(config)# wlan testwprofile 22 ssid-3`	Configures the WLAN and SSID.
Step 3	**security dot1x authentication-list** *default* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Configures 802.1X for an WLAN.
Step 4	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for 802.1x security on the WLAN.
Step 5	**security web-auth parameter-map** *global* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Configures the global parameter map.
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring Local Web Authentication with PSK Protocol

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile wlan-id ssid* **Example:** `Device(config)# wlan psksec-profile 22 ssid-4`	Configures the WLAN and SSID.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.

	Command or Action	Purpose
Step 4	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**security wpa psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Enables the security type as PSK.
Step 7	**security wpa psk set-key** {*ascii* | *hex*} *key* **Example:** `Device(config-wlan)# security wpa akm psk set-key asci 0`	Configures the PSK shared key.
Step 8	**security web-auth** **Example:** `Device(config-wlan)# security web-auth`	Enables the web authentication for the WLAN.
Step 9	**security web-auth authentication-list** *default* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for the WLAN.
Step 10	**security web-auth parameter-map** *global* **Example:** `Device(config-wlan)# security web-auth parameter-map global`	Configure the global parameter map.

Central Web Authentication with PSK Protocol

To configure the CWA with PSK security protocol, follow the steps:

1. Configure WLAN Profile for Central Web Authentication with PSK Protocol
2. Applying Policy Profile on a WLAN

Configure WLAN Profile for Central Web Authentication with PSK Protocol

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile wlan-id ssid* **Example:** `Device(config)# wlan cwasec-profile 27 ssid-5`	Configures the WLAN and SSID.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 4	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**security wpa psk** **Example:** `Device(config-wlan)# security wpa psk`	Enables the security type as PSK.
Step 7	**security wpa psk set-key** {*ascii* | *hex*} *key* **Example:** `Device(config-wlan)# security wpa psk set-key asci 0`	Configures the PSK shared key.
Step 8	**mac-filtering** *authorization_list_name* **Example:** `Device(config-wlan)# mac-filtering cwa-list`	Enables MAC filtering for PSK web authentication.

Central Web Authentication with iPSK Protocol

To configure the CWA with iPSK security protocol, follow the steps:

1. Configure WLAN Profile for Central Web Authentication with iPSK Protocol

Configure WLAN Profile for Central Web Authentication with iPSK Protocol

Procedure

	Command or Action	Purpose
Step 1	**wlan** *guest-wlan-name wlan-id ssid* **Example:** `config# wlan ipsk-cwa-profile 28 ssid-6`	Configures guest WLAN.
Step 2	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for 802.1x.
Step 3	**security wpa akm psk set-key** {*ascii* | *hex*} *key* **Example:** `Device(config-wlan)# security wpa akm psk set-key asci 0`	Configures the PSK AKM shared key.
Step 4	**mac-filtering** *authorization_list_name* **Example:** `Device(config-wlan)# mac-filtering cwa-list`	Enables MAC filtering for iPSK authentication.

Configure Web Authentication on MAC Address Bypass failure (GUI)

Procedure

Step 1 Click **Configuration** > **Tags and Profiles** > **WLANs**.

Step 2 Click **Add** to add a new WLAN Profile or click the one you want to edit.

Step 3 In the **Edit WLAN** window, complete the following steps:

a) Choose **Security** > **Layer2** and check the **MAC Filtering** check box to enable MAC filtering.

b) From the **Authorization List** drop-down list, select a value.

c) Choose the **Layer3** tab.

d) Click **Show Advanced Settings** and check the **On MAC Filter Failure** checkbox.

Configure Web Authentication on MAC Address Bypass Failure (CLI)

You can configure authentication to fall back to web authentication, if a client cannot authenticate using MAC filter (Local or RADIUS), while trying to connect to a WLAN. To enable this feature, configure both MAC filtering and Web Authentication on the device. This can also avoid disassociations that happen only because of MAC filter authentication failure. To configure this feature, follow the procedure:

Configure a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy cwa`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Enables Central switching.

Step 4	Choose the first option to configure a Guest Foreign or second option to configure a Guest Anchor:
	• **mobility anchor** *anchor-ip-address*
	• **mobility anchor**
	Example:
	For Guests Foreign:
	`Device (config-wireless-policy)# mobility anchor 19.0.2.1`
	For Guest Anchor:
	`Device (config-wireless-policy)# mobility anchor`
		Configures Guest Foreign or Guest Anchor.

Step 5	**vlan** *name* **Example:** `Device(config-wireless-policy)# vlan 16`	Configures a VLAN name or VLAN ID. **Note** VLAN is optional for a Guest Foreign controller.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

Configure a WLAN Profile

Procedure

	Command or Action	Purpose
Step 1	**wlan** *guest-wlan-name wlan-id ssid* **Example:** `config# wlan test-wlan-guest 10 wlan-ssid`	Configures guest WLAN.
Step 2	**mac-filtering** *mac-auth-listname* **authorization-override** *override-auth-listname* **Example:** `config-wlan# mac-filtering mac-auth-listname authorization-override`	Configures MAC filtering support on WLAN.
Step 3	**security web-auth** **Example:** `config-wlan# security web-auth`	Enables web authentication.
Step 4	**security web-auth on-macfilter-failure** **Example:** `config-wlan# security web-auth on-macfilter-failure`	Enables web authentication if MAC filter authentication fails.

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Pre-Shared Key (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters.

	Command or Action	Purpose
		Note If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**security wpa psk set-key** *ascii/hex key password* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	Configures the PSK AKM shared key.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK support.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

	Command or Action	Purpose
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with OWE (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 6	**security wpa akm owe** **Example:**	Enables WPA3 OWE support.

	Command or Action	Purpose
	`Device(config-wlan)# security wpa akm owe`	
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Secure Agile Exchange (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN.

	Command or Action	Purpose
		• *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter the **wlan** *profile-name* command.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 6	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 7	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables authentication list for dot1x security.
Step 8	**security web-auth authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security web-auth authorization-list default`	Enables authorization list for dot1x security.
Step 9	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 10	**security web-auth parameter-map** *parameter-map-name*	Configures the parameter map.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	**Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring WLAN for Web Authentication on MAC Authentication Failure with Dot1x (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id SSID_Name* **Example:** `Device(config)# wlan wlan-test 3 ssid-test`	Enters WLAN configuration submode. • *profile-name*: Profile name of the configured WLAN. • *wlan-id*: Wireless LAN identifier. Range is from 1 to 512. • *SSID_Name*: SSID that can contain 32 alphanumeric characters. **Note** If you have already configured a WLAN, enter the profile name of the configured WLAN in the command (**wlan** *profile-name*) and continue with the rest of the configuration steps.
Step 3	**mac-filtering** *auth-list-name* **Example:** `Device(config-wlan)# mac-filtering test-auth-list`	Sets the MAC filtering parameters.
Step 4	**security dot1x authentication-list** *dot1x-authentication-list* **Example:**	Configures 802.1x.

	Command or Action	Purpose
	`Device(config-wlan)# security dot1x authentication-list dot1x-authentication-list`	
Step 5	**security web-auth authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security web-auth authentication-list default`	Enables the authentication list.
Step 6	**security web-auth on-macfilter-failure** **Example:** `Device(config-wlan)# security web-auth on-macfilter-failure`	Enables web authentication on MAC filter failure.
Step 7	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	Configures the web authentication parameter map. **Note** If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

CHAPTER 183

Wired Guest Access

- Information About Wired Guest Access, on page 2047
- Restrictions for Wired Guest Access, on page 2050
- Configuring Access Switch for Wired Guest Client, on page 2050
- Configuring Access Switch for Foreign Controller, on page 2051
- Configuring Foreign Controller with Open Authentication (GUI), on page 2052
- Configuring Foreign Controller with Open Authentication, on page 2052
- Configuring Foreign Controller with Local Web Authentication (GUI), on page 2054
- Configuring Foreign Controller with Local WEB Authentication, on page 2055
- Configuring Anchor Controller with Open Authentication (GUI), on page 2056
- Configuring Anchor Controller with Open Authentication, on page 2057
- Configuring Anchor Controller with Local Web Authentication (GUI), on page 2058
- Configuring Anchor Controller with Local Web Authentication, on page 2059
- Configuring Session Timeout for a Profile Policy, on page 2060
- Global Configuration (GUI), on page 2061
- Verifying Wired Guest Configurations, on page 2061
- Wired Guest Access—Use Cases, on page 2065

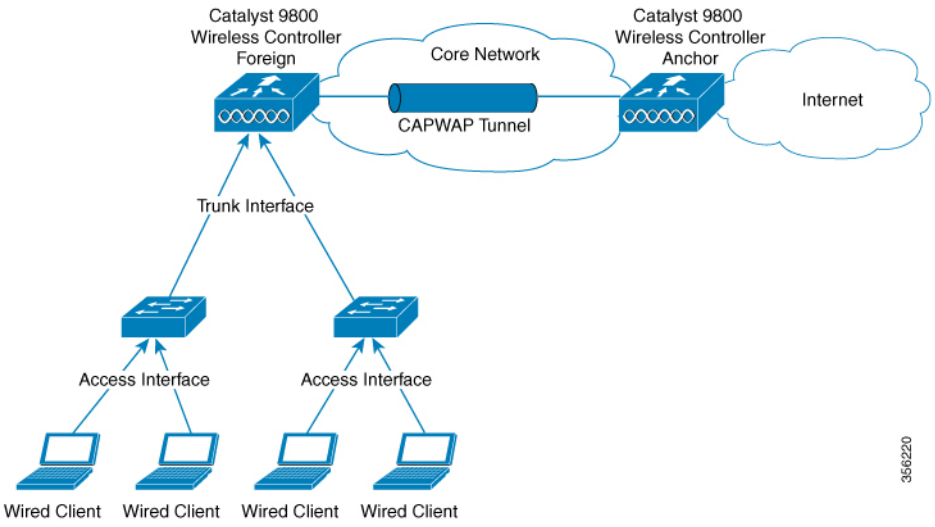
Information About Wired Guest Access

The Wired Guest Access feature enables guest users of an enterprise network that supports both wired and wireless access to connect to the guest access network. The wired guest clients can connect from the designated and configured wired Ethernet ports for the guest access after they complete the configured authentication methods. Wired session guests are directed to a wireless guest controller in a demilitarized zone (DMZ) through a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel.

Wired guest access can be configured in a dual-controller configuration that uses both an anchor controller and a foreign controller. A dual-controller configuration isolates wired guest access traffic from the enterprise user traffic.

The wired session guests are provided open or web-authenticated access from the wireless controller.

Figure 54: Guest Access Architecture



IPv6 Router Advertisement Forwarding for a Wired Guest

Wired clients get the IPv6 based connectivity when they receive the IPv6 Router Advertisement (RA) message. The IPv6 router sends these RA messages and it contains information such as IPv6 prefix and router link-local address.

These RA messages are sent as Unicast or Multicast messages. The Unicast RA messages are routed as same as the client directed traffic. The Multicast RA messages are forwarded to all the clients present in the intended VLAN. RA message forwarding is enabled by default and requires no specific configuration.

Guest Anchor Controller: Guest anchor controller forwards the RA packets, from the receiving VLAN, to all the foreign controllers using the mobility data tunnel. The RA packets are tagged with the anchor VLAN to ensure the message is forwarded to the correct clients using the foreign controller data path.

Guest Foreign Controller: Guest foreign controller forwards the received RAs from the guest anchor to the wired ports on which the wired guest clients are connected. To forward the RAs to the intended clients, the guest foreign controller keeps a track of the wired guest clients–per interface, access VLANs, and anchor VLANs.

Supported Features

- Cisco Catalyst 9800 Series Wireless Controllers-Anchor
- Cisco AireOS Wireless Controllers-Anchor
- Cisco Catalyst 9800 Series Wireless Controllers-Foreign
- Cisco AireOS Wireless Controllers-Foreign
- Dual controller solution (foreign + anchor) and access switch
- Trunk Ports
- Open Authentication
- Local Web Authentication

To configure Web Authentication, see Web-based Authentication section of the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

- Local Web Authentication (web consent).

Note In AireOS, this is referred to as **web pass-through**.

- Local Web Authentication + ISE (External Web Authentication).
- LWA (local web authentication), with a username and a password.
- Web consent (LWA + consent), that is with a username, a password and the check box of acceptance.

- Scale max 2k clients and 5 guest-LANs (5 VLANs max)
- Client IPv6 support
- Idle Timeout and Session Timeout
- Accounting on Foreign

Note Statistics computation not supported.

- Manageability (SNMP/Yang/WebUI)
- QoS Rate-Limiting and MQC Policies (Upstream at foreign, Upstream, and Downstream at the anchor)

Note QoS rate-limiting supports bps rate-limiting, pps rate-limiting is not supported.

- QoS support with AireOS Anchor setup
- Stateful Switch Over (SSO)
- Port Channel support on Anchor and Foreign with no restrictions to the controller's role.
- Access Port on Foreign
- Cisco Umbrella (not supported in AireOS Anchor)
- ACL support at anchor
- Fully Qualified Domain Name (FQDN) URL filtering is supported at Anchor controller.
- IP theft detection
- Sleeping Client

Restrictions for Wired Guest Access

- A maximum of five guest LANs are supported on the foreign controller.
- A maximum of 2000 clients per foreign are supported.
- No Multicast or Broadcast support.
- You can map only one wired VLAN to a guest LAN.
- You can map only one guest LAN to one policy profile.
- Every guest LAN has a unique name and this name cannot be shared with RLAN or WLAN.
- Ensure that the Anchor VLAN ID and the wired VLAN ID configured on the Foreign controller is not the same.
- QoS is not supported on VLAN and on physical interfaces of the controller.

Configuring Access Switch for Wired Guest Client

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan** *vlan-id* **Example:** `Device(config)#vlan 200`	Creates the VLAN ID.
Step 3	**exit** **Example:** `Device(config)#exit`	Returns to configuration mode.
Step 4	**interface GigabitEthernet***interface number* **Example:** `Device(config)#interface GigabitEthernet1/0/1`	Enters the interface to be added to the VLAN.
Step 5	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)#switchport access vlan 200`	Assigns the port to a VLAN. The valid VLAN IDs range is between 1 and 4094.

	Command or Action	Purpose
Step 6	**switchport mode access** **Example:** `Device(config-if)#switchport mode access`	Defines the VLAN membership mode for the port.
Step 7	**no cdp enable** **Example:** `Device(config-if)#no cdp enable`	Disables CDP on the interface.
Step 8	**end** **Example:** `Device(config-if)#end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

Configuring Access Switch for Foreign Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan** *vlan-id* **Example:** `Device(config)#vlan 200`	Creates the VLAN ID.
Step 3	**exit** **Example:** `Device(config)#exit`	Returns to configuration mode.
Step 4	**interface GigabitEthernet***interface number* **Example:** `Device(config)#interface GigabitEthernet1/0/2`	Enters the interface to be added to the VLAN.
Step 5	**switchport trunk allowed vlan** *vlan-id* **Example:** `Device(config-if)#switchport trunk allowed vlan 200`	Assigns the allowed VLAN ID to the port when it is in trunking mode.
Step 6	**switchport mode trunk** **Example:** `Device(config-if)#switchport mode trunk`	Sets the trunking mode to trunk unconditionally.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-if)#end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.

Configuring Foreign Controller with Open Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Click on a **Policy Name**.
Step 3 Go to the **Mobility** tab.
Step 4 In the **Mobility Anchors** section, check the **Export Anchor** check box.
Step 5 Click **Apply to Device**.
Step 6 Choose **Configuration** > **Wireless** > **Guest LAN** > **Guest LAN Configuration**
Step 7 Click **Add**.
Step 8 In the **General** tab, enter the **Profile Name**, **Guest LAN ID**, **Client Association Limit**.
Step 9 Choose the desired mode from the **mDNS Mode** drop-down list.
Step 10 Enable or disable the **Status** and **Wired VLAN Status** toggle button.
Step 11 In the **Security** tab, disable the **Web Auth** toggle button.
Step 12 Click **Apply to Device**.
Step 13 Choose **Configuration** > **Wireless** > **Guest LAN** > **Guest LAN Map Configuration**
Step 14 Click **Add Map**.
Step 15 In the Add Guest LAN Map window, enter the **Guest LAN Map**.
Step 16 Click **Apply to Device**.
Step 17 Click **Add**.
Step 18 Choose the values from the **Profile Name** and **Policy Name** drop-down lists.
Step 19 Click **Save**.

Configuring Foreign Controller with Open Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)#wireless profile policy testpro-1`	Configures the WLAN policy profile.
Step 3	**mobility anchor** *non-local-mobility-cntlr-ip* **priority** *priority* **Example:** `Device(config-wireless-policy)#mobility anchor 192.168.201.111 priority 1`	Configures the mobility anchor and sets its priority.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)#no shutdown`	Enables the configuration.
Step 5	**exit** **Example:** `Device(config-wireless-policy)#exit`	Returns to configuration mode.
Step 6	**guest-lan profile-name** *guest-profile-name guest-lan-id* **wired-vlan** *wired-vlan-id* **Example:** `Device(config)#guest-lan profile-name gstpro-1 1 wired-vlan 25`	Configures guest LAN profile with a wired VLAN. **Note** Configure the wired VLAN only for the Guest Foreign controller.
Step 7	**no security web-auth** **Example:** `Device(config-guest-lan)#no security web-auth`	Disables web-authentication.
Step 8	**no shutdown** **Example:** `Device(config-guest-lan)#no shutdown`	Enables the guest LAN.
Step 9	**exit** **Example:** `Device(config-guest-lan)#exit`	Returns to configuration mode.
Step 10	**wireless guest LAN map** *gst-map-name* **Example:** `Device(config)#wireless guest LAN map gstmap-1`	Configures a guest LAN map.

	Command or Action	Purpose
Step 11	**guest-lan** *guest-profile-name* **policy** *wlan-policy-profile-name* **Example:** `Device(config-guest-lan-map)#guest-lan gstpro-1 policy testpro-1`	Attaches a guest LAN map to the policy profile.
Step 12	**exit** **Example:** `Device(config-guest-lan-map)#exit`	Returns to configuration mode.

Configuring Foreign Controller with Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Select a **Policy Name**.
Step 3 Go to the **Mobility** tab.
Step 4 In the **Mobility Anchors** section, check the **Export Anchor** check box.
Step 5 Click **Update & Apply to Device**.
Step 6 Choose **Configuration** > **Wireless** > **Guest LAN** > **Guest LAN Configuration**
Step 7 Click **Add**.
Step 8 In the **General** tab, enter the **Profile Name**, **Guest LAN ID**, **Client Association Limit**.
Step 9 Choose the desired mode from the **mDNS Mode** drop-down list.
Step 10 Enable or disable the **Status** and **Wired VLAN Status** using toggle button.
Step 11 Go to the **Security** tab.
Step 12 Enable the **Web Auth** using toggle button.
Step 13 Choose the values from the **Web Auth Parameter Map**, **Authentication List** and **Authorization List** drop-down lists.
Step 14 Click **Apply to Device**.
Step 15 Choose **Configuration** > **Wireless** > **Guest LAN** > **Guest LAN Map Configuration**
Step 16 Click **Add Map**.
Step 17 In the Add Guest LAN Map window, enter the **Guest LAN Map**.
Step 18 Click **Apply to Device**.
Step 19 Click **Add**.
Step 20 Choose the values from the **Profile Name** and **Policy Name** drop-down lists.
Step 21 Click **Save**.

Configuring Foreign Controller with Local WEB Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)#wireless profile policy testpro-1`	Configures the WLAN policy profile.
Step 3	**mobility anchor** *non-local-mobility-cntlr-ip* **priority** *priority* **Example:** `Device(config-wireless-policy)#mobility anchor 192.168.201.111 priority 1`	Configures the mobility anchor and sets its priority.
Step 4	**no shutdown** **Example:** `Device(config-wireless-policy)#no shutdown`	Enables the configuration.
Step 5	**exit** **Example:** `Device(config-wireless-policy)#exit`	Returns to configuration mode.
Step 6	**guest-lan profile-name** *guest-profile-name guest-lan-id* **wired-vlan** *wired-vlan-id* **Example:** `Device(config)#guest-lan profile-name gstpro-2 3 wired-vlan 26`	Configures guest LAN profile with a wired VLAN.
Step 7	**security web-auth** **Example:** `Device(config-guest-lan)#security web-auth`	Enables web-authentication.
Step 8	**security web-auth authentication-list** *auth-list-name* **Example:** `Device(config-guest-lan)#security web-auth authentication-list default`	Configures the authentication list for a IEEE 802.1x network.

	Command or Action	Purpose
Step 9	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-guest-lan)#security web-auth parameter-map global`	Configures the security web-auth parameter map.
Step 10	**no shutdown** **Example:** `Device(config-guest-lan)#no shutdown`	Enables the guest LAN.
Step 11	**exit** **Example:** `Device(config-guest-lan)#exit`	Returns to configuration mode.
Step 12	**wireless guest-lan map** *gst-map-name* **Example:** `Device(config)#wireless guest-lan map gstmap-2`	Configures a guest LAN map.
Step 13	**guest-lan** *guest-lan-profile-name* **policy** *policy-profile-name* **Example:** `Device(config-guest-lan-map)#guest-lan gstpro-2 policy testpro-1`	Attaches a guest LAN map to the policy profile.
Step 14	**exit** **Example:** `Device(config-guest-lan-map)#exit`	Returns to configuration mode.

What to do next

For more information about Local Web Authentication, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/wireless-web-authentication.html

Configuring Anchor Controller with Open Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name**.

Step 4 Go to the **Access Policies** tab.

Step 5 Under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list.

Step 6 Go to the **Mobility** tab.

Step 7 Under the **Mobility Anchors** settings, check the **Export Anchor** check box.

Step 8 Click **Apply to Device**.

Step 9 Choose **Configuration** > **Wireless** > **Guest LAN**.

Step 10 Click **Add**.

Step 11 In the **General** tab, enter the **Profile Name**, the **Guest LAN ID** and the **Client Association Limit**.

Step 12 In the **Security** tab, under the **Layer3** settings, disable the **Web Auth** toggle button.

Step 13 Click **Apply to Device**.

Configuring Anchor Controller with Open Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)#wireless profile policy testpro-2`	Configures the WLAN policy profile.
Step 3	**mobility anchor** **Example:** `Device(config-wireless-policy)#mobility anchor`	Configures the mobility anchor.
Step 4	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)#vlan 29`	Configure a VLAN name or a VLAN ID.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)#no shutdown`	Enables the configuration.
Step 6	**exit** **Example:** `Device(config-wireless-policy)#exit`	Returns to configuration mode.

	Command or Action	Purpose
Step 7	**guest-lan profile-name** *guest-profile-name guest-lan-id* **Example:** `Device(config)#guest-lan profile-name testpro-2 1`	Configures the guest LAN profile with a wired VLAN.
Step 8	**client association limit** *guest-lan-client-limit* **Example:** `Device(config-guest-lan)#client association limit`	Configures the maximum client connections per guest LAN. The valid range is between 1 and 2000.
Step 9	**no security web-auth** **Example:** `Device(config-guest-lan)#no security web-auth`	Disables web authentication.
Step 10	**no shutdown** **Example:** `Device(config-guest-lan)#no shutdown`	Enables the guest LAN.
Step 11	**exit** **Example:** `Device(config-guest-lan)#exit`	Returns to configuration mode.

Configuring Anchor Controller with Local Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.
Step 2 Click **Add**.
Step 3 In the **General** tab, enter the **Name**.
Step 4 Go to the **Access Policies** tab.
Step 5 Under the **VLAN** settings, choose the vlans from the **VLAN/VLAN Group** drop-down list.
Step 6 Go to the **Mobility** tab.
Step 7 Under the **Mobility Anchors** settings, check the **Export Anchor** check box.
Step 8 Click **Apply to Device**.
Step 9 Choose **Configuration** > **Wireless** > **Guest LAN**.
Step 10 Click **Add**.
Step 11 In the **General** tab, enter the **Profile Name**, the **Guest LAN ID** and the **Client Association Limit**.

Step 12 In the **Security** tab, under the **Layer3** settings, enable the **Web Auth** toggle button. Choose the Parameter map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.

Step 13 Click **Apply to Device**.

Configuring Anchor Controller with Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name* **Example:** `Device(config)#wireless profile policy testpro-2`	Configures the WLAN policy profile.
Step 3	**mobility anchor** **Example:** `Device(config-wireless-policy)#mobility anchor`	Configures the mobility anchor.
Step 4	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)#vlan 30`	Configure a VLAN name or a VLAN ID.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)#no shutdown`	Enables the configuration.
Step 6	**exit** **Example:** `Device(config-wireless-policy)#exit`	Returns to configuration mode.
Step 7	**guest-lan profile-name** *guest-profile-name guest-lan-id* **Example:** `Device(config)#guest-lan profile-name testpro-2 1`	Configure a guest LAN profile with a wired VLAN.

	Command or Action	Purpose
Step 8	**client association limit** *guest-lan-client-limit* **Example:** `Device(config-guest-lan)#client association limit`	Configures the maximum client connections per guest LAN. The valid range is between 1 and 2000.
Step 9	**security web-auth** **Example:** `Device(config-guest-lan)#security web-auth`	Configures web authentication.
Step 10	**security web-auth parameter-map** *parameter-map-name* **Example:** `Device(config-guest-lan)#security web-auth parameter-map testmap-1`	Configures the security web-auth parameter map.
Step 11	**security web-auth authentication-list** *authentication-list-name* **Example:** `Device(config-guest-lan)#security web-auth authentication-list testlwa-1`	Configures the authentication list for the IEEE 802.1x network.
Step 12	**no shutdown** **Example:** `Device(config-guest-lan)#no shutdown`	Enables the guest-LAN.
Step 13	**exit** **Example:** `Device(config-guest-lan)#exit`	Returns to configuration mode.

Configuring Session Timeout for a Profile Policy

Session Timeout for a wired guest is set to infinite by default. Perform the following procedure to configure the timeout values to the wired guest.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *wlan-policy-profile-name*	Configures the WLAN policy profile.

	Command or Action	Purpose
	Example: `Device(config)#wireless profile policy testpol-1`	
Step 3	**guest-lan enable-session-timeout** **Example:** `Device(config-wireless-policy)#guest-lan enable-session-timeout`	Enables the client session timeout on the guest LAN.
Step 4	**session-timeout** *timeout-duration* **Example:** `Device(config-wireless-policy)#session-timeout 1000`	Configures the client session timeout in seconds. The valid range is between 0 and 86400 seconds.

Global Configuration (GUI)

Procedure

Step 1 Choose **Administration** > **User Administration**.

Step 2 Click **Add**.

Step 3 Enter the **Username**, **Password** and **Confirm Password**.

Step 4 Choose the desired value from the **Policy** and **Privilege** drop-down lists.

Step 5 Click **Apply to Device**.

Step 6 Choose **Administration** > **Management** > **HTTP/HTTPS/Netconf**.

Step 7 In the **HTTP/HTTPS Access Configuration** settings, enable or disable the **HTTP Access**, **HTTPS Access** and **Personal Identity Verification** toggle buttons.

Step 8 Enter the **HTTP Port** and **HTTPS Port**.

Step 9 Click **Apply**.

Verifying Wired Guest Configurations

To validate the wireless configuration, use the following command:

```
Device# wireless config validate

Wireless Management Trustpoint Name: 'WLC-29c_WLC_TP'
        Trustpoint certificate type is WLC-SSC
    Wireless management trustpoint config is valid

Jan 22 07:49:15.371: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
Error in No record found for VLAN 9, needed by Guest-LAN open-wired
```

To display the summary of all Guest-LANs, use the following command:

```
Device# show guest-lan summary

Number of Guest LANs: 1

GLAN  GLAN Profile Name                 Status
-----------------------------------------
1     wired_guest_open                  UP
```

To view the detailed output of all Guest-LANs, use the following command:

```
Device# show guest-lan all

Guest-LAN Profile Name     : open
================================================
Guest-LAN ID                                  : 1
Wired-Vlan                                    : 200
Status                                        : Enabled
Number of Active Clients                      : 1
Max Associated Clients                        : 2000
Security
    WebAuth                                   : Enabled
    Webauth Parameter Map                     : global
    Webauth Authentication List               : LWA-AUTHENTICATION
    Webauth Authorization List                : LWA-AUTHENTICATION
```

To view the guest-LAN configuration by ID, use the following command:

```
Device# show guest-lan id 1
Guest-LAN Profile Name     : open
================================================
Guest-LAN ID                                  : 1
Wired-Vlan                                    : 200
Status                                        : Enabled
Number of Active Clients                      : 1
Max Associated Clients                        : 2000
Security
    WebAuth                                   : Enabled
    Webauth Parameter Map                     : global
    Webauth Authentication List               : LWA-AUTHENTICATION
    Webauth Authorization List                : LWA-AUTHENTICATION
```

To view the guest-LAN configuration by profile name, use the following command:

```
Device# show guest-lan name open

Guest-LAN Profile Name     : open
================================================
Guest-LAN ID                                  : 1
Wired-Vlan                                    : 200
Status                                        : Enabled
Number of Active Clients                      : 1
Max Associated Clients                        : 2000
Security
    WebAuth                                   : Enabled
    Webauth Parameter Map                     : global
    Webauth Authentication List               : LWA-AUTHENTICATION
    Webauth Authorization List                : LWA-AUTHENTICATION
```

To view the guest-LAN map summary, use the following command:

```
Device# show wireless guest-lan-map summary

Number of Guest-Lan Maps: 2

WLAN Profile Name                Policy Name
------------------------------------------------------------------------
open_wired_guest                 open_wired_guest
lwa_wired_guest                  lwa_wired_guest
```

To view the active clients, use the following command:

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                                          Type ID   State
Protocol Method     Role
-------------------------------------------------------------------------------------------------------------------
000a.bd15.0001 N/A                                              GLAN 1    Run
802.3    Web Auth   Export Foreign
```

To view the detailed information about a client by MAC address, use the following command:

```
Device# show wireless client mac-address 3383.0000.0001 detail

Client MAC Address : 3383.0000.0001
Client IPv4 Address : 155.165.152.151
Client Username: N/A
AP MAC Address:  N/A
AP slot : N/A
Client State : Associated
Policy Profile : guestlan_lwa
Flex Profile : N/A
Guest Lan:
  GLAN Id: 2
  GLAN Name: guestlan_lwa
  Wired VLAN: 312
Wireless LAN Network Name (SSID) : N/A
BSSID : N/A
Connected For : 128 seconds
Protocol : 802.3
Channel : N/A
Client IIF-ID : 0xa0000002
Association Id : 0
Authentication Algorithm : Open System
Session Timeout : 1800 sec (Timer not running)
Session Warning Time : Timer not running
Input Policy Name  : clsilver
Input Policy State : Installed
Input Policy Source : AAA Policy
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 0 (kbps)
  QoS Realtime Average Data Rate Upstream    : 0 (kbps)
  QoS Burst Data Rate Upstream               : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
  QoS Average Data Rate Downstream           : 0 (kbps)
```

```
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Anchor IP Address          : 101.0.0.1
  Point of Attachment        : 0x00000008
  Point of Presence          : 0xA0000001
  AuthC status               : Enabled
  Move Count                 : 0
  Mobility Role              : Export Foreign
  Mobility Roam Type         : L3 Requested
  Mobility Complete Timestamp : 05/07/2019 22:31:45 UTC
Client Join Time:
  Join Time Of Client : 05/07/2019 22:31:42 UTC
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 125 seconds
Policy Type : N/A
Encryption Cipher : N/A
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : default
Multicast VLAN : 0
Access VLAN : 153
Anchor VLAN : 155
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Point of Attachment : TenGigabitEthernet0/0/0
  IIF ID             : 0x00000008
  Authorized         : TRUE
  Session timeout    : 1800
  Common Session ID: 00000000000000CB946C8BA3
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
   Server IP :
  Auth Method Status List
   Method : Web Auth
    Webauth State    : Authz
    Webauth Method   : Webauth
  Local Policies:
   Service Template : wlan_svc_guestlan_lwa_local (priority 254)
    VLAN             : 153
    Absolute-Timer   : 1800
  Server Policies:
    QOS Level        : 0
  Resultant Policies:
    VLAN Name         : VLAN0153
    QOS Level        : 0
    VLAN             : 153
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
```

```
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received : 0
  Number of Bytes Sent : 0
  Number of Packets Received : 8
  Number of Packets Sent : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
  Idle time : 0 seconds
  Last idle time update : 05/07/2019 22:32:27
  Last statistics update : 05/07/2019 22:32:27
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : Pending Classification
```

Wired Guest Access—Use Cases

This feature while performing as a guest access feature can be used to meet different requirements. Some of the possibilities are shared here.

Scenario One–Equipment Software Update

This feature can be configured to allow the wired port to connect to the manufacture or vendor website for equipment maintenance, software, or firmware updates.

Scenario Two–Video Streaming

This feature can be configured to allow devices that are connected to a wired port to stream video to visitor information screens.

CHAPTER 184

Express Wi-Fi by Facebook

- Information About Express Wi-Fi by Facebook, on page 2067
- Restrictions for Express Wi-Fi by Facebook, on page 2068
- Enabling Express Wi-Fi by Facebook NAC for Policy Profile (GUI), on page 2068
- Enabling Accounting RADIUS Server for Flex Profile (GUI), on page 2069
- Configuring Captive Portal for Express Wi-Fi by Facebook (GUI), on page 2069
- Configuring Captive Portal for Express Wi-Fi by Facebook (CLI), on page 2069
- Configuring Express Wi-Fi by Facebook Policy on Controller (CLI), on page 2070
- Configuring RADIUS Server for Accounting and Authentication in FlexConnect Profile (CLI), on page 2072
- Verifying Express Wi-Fi by Facebook Configurations on Controller, on page 2073
- Verifying Express Wi-Fi by Facebook Configurations on the AP, on page 2073

Information About Express Wi-Fi by Facebook

Express Wi-Fi by Facebook is a cloud-based, low-cost solution for local entrepreneurs and SMBs in emerging countries to provide Wi-Fi access. Using Express Wi-Fi by Facebook, users can buy data packs and find nearby hotspots.

Facebook provides the software (and sometimes hardware) infrastructure while the ISP or SMB provides internet connectivity and deployments to the subscribers. These service providers provision guest access through a captive portal. This can include both free and paid services including paid internet access with quota enforcement.

Express Wi-Fi by Facebook feature is enabled through a FlexConnect deployment based on the cloud-hosted Cisco Catalyst 9800 Series Wireless Controller where the Cisco AP performs client-related functions such as web authentication, captive portal redirect, matching and accounting of traffic classes and connection to the RADIUS server. This feature also supports FQDN (DNS ACLs) and IP ACLs as well as MAC authentication on the AP. The controller provisions the AP with the required configuration for these tasks.

Note If an AP reboots in standalone mode, the flexconnect URL ACL is not retained. This will cause Express Wi-Fi by Facebook to stop working.

The Express Wi-Fi by Facebook solution comprises the following components:

- Cisco Catalyst 9800 Series Wireless Controller

- Cisco Aironet Wave 2 or Catalyst APs
- Facebook infrastructure

Restrictions for Express Wi-Fi by Facebook

- Express Wi-Fi by Facebook is supported only in a FlexConnect deployment with local switching, local authentication, and local association.
- Express Wi-Fi by Facebook is supported only on Cisco Aironet Wave 2 and Catalyst access points.
- Only three traffic classes are supported.
- The AP supports only three ACLs per client.
- All APs forming a roaming domain should have Layer 2 reachability.
- Up to 64 complex rules and 512 simple rules per ACL are supported, where a simple rule comprises of a destination IP address and port. A complex rule contains more than a destination IP address and port information.
- Only RADIUS CoA messages with the Facebook attribute are supported on the AP.

Enabling Express Wi-Fi by Facebook NAC for Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy** page, click the name of the desired Policy Profile.

Step 3 In the **Edit Policy Profile** window, click the **Advanced** tab.

Step 4 In the **AAA Policy** section, enable the **AAA override** . The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Step 5 Enable the **NAC State** check box to enable Cisco Network Admission Control (NAC).

Note You can enable NAC state only when AAA override is enabled.

Step 6 From the **NAC Type** drop-down list, select the type of NAC. The default is *XWF*.

Step 7 From the **Policy Name** drop-down list, choose a policy name.

Step 8 From the **Accounting List** drop-down list, choose an accounting list.

Step 9 Enable **Interim Accounting** to maintain a session with NAC.

Step 10 Click **Update & Apply to Device**.

Enabling Accounting RADIUS Server for Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.
Step 2 On the Flex page, click the name of the desired Flex Profile.
Step 3 In the **Edit Flex Profile** window, click the **Local Authentication** tab.
Step 4 Choose the desired server group from the **Local Accounting RADIUS Server Group** drop-down list.
Step 5 Select the **Local Client Roaming** check box.
Step 6 Click **Update & Apply to Device**.

Configuring Captive Portal for Express Wi-Fi by Facebook (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.
Step 2 On the **Web Auth** page, click the name of the desired parameter map.
Step 3 In the **Edit Web Auth Parameter** window, click the **Advanced** tab.
Step 4 In the **Redirect to External Server** section, select the **Express Wi-Fi Key Type** from the drop-down list.
Step 5 Enter the vendor specific key in the **Express Wi-Fi Key** field.
Step 6 Click **Update & Apply to Device**.

Configuring Captive Portal for Express Wi-Fi by Facebook (CLI)

Before you begin

- Configure the URL filter list.
- Configure the IP ACL.

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**parameter-map type webauth** *parameter-map- name* **Example:** `Device(config)# parameter-map type webauth FACEBOOK-MAP`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 3	**type webauth** **Example:** `Device(config-params-parameter-map)# type webauth`	Configures the webauth type parameter.
Step 4	**redirect for-login** *url-string* **Example:** `Device(config-params-parameter-map)# redirect for-login https://xwfcisco-us.expresswifi.com/customer/captive_portal`	Configures the URL string for redirection during login.
Step 5	**captive-bypass-portal** **Example:** `Device(config-params-parameter-map)# captive-bypass-portal`	Configures captive bypassing.
Step 6	**redirect vendor-specific xwf key 0** *vendor-key* **Example:** `Device(config-params-parameter-map)# redirect vendor-specific xwf key 0 vendor-key`	Configures the URL string for redirection during login.
Step 7	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring Express Wi-Fi by Facebook Policy on Controller (CLI)

Before you begin

- Enable web authentication and MAC filtering on the WLAN.
- Configure RADIUS proxy server and accounting server.

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy default-policy- profile`	Configures the wireless profile policy.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa override`	Configures AAA override to apply policies coming from the AAA or ISE servers.
Step 4	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Disables central switching and enables local switching.
Step 5	**no central association** **Example:** `Device(config-wireless-policy)# no central association`	Disables central association and enables local association for locally switched clients.
Step 6	**no central authentication** **Example:** `Device(config-wireless-policy)# no central authentication`	Disables central authentication and enables local authentication.
Step 7	**nac xwf** **Example:** `Device(config-wireless-policy)# nac xwf`	Configures NAC in the policy profile.
Step 8	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 9`	Configures a VLAN name or VLAN ID.
Step 9	**no shutdown** **Example:**	Enables the profile policy.

	Command or Action	Purpose
	`Device(config-wireless-policy)# no shutdown`	
Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring RADIUS Server for Accounting and Authentication in FlexConnect Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex default-flex- profile`	Configures the wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**local-auth radius-server-group** *group-name* **Example:** `Device(config-wireless-flex-profile)# local-auth radius-server-group FB_GROUP`	Configures the authentication server group name.
Step 4	**local-accounting radius-server-group** *group-name* **Example:** `Device(config-wireless-flex-profile)# local-accounting radius-server-group group-name`	Configures the accounting server group name.
Step 5	**local-roaming** **Example:** `Device(config-wireless-flex-profile)# local-roaming`	Enables local roaming.
Step 6	**acl-policy** *policy-name* **Example:**	Configures ACL policy.

	Command or Action	Purpose
	`Device(config-wireless-flex-profile)# acl-policy fbs`	
Step 7	**urlfilter list** *list-name* **Example:** `Device(config-wireless-flex-profile)# urlfilter list fbs`	Applies the URL list to the Flex profile. Here, *list-name* refers to the URL filter list name. The list name must not exceed 32 alphanumeric characters. Note: For a given traffic class, the *list-name* should match the above ACL *policy-name*.
Step 8	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Returns to privileged EXEC mode.

Verifying Express Wi-Fi by Facebook Configurations on Controller

To view ACLs applied on a specific client and the associated AP's MAC address, use the following command:

```
Device# show wireless client mac-address 0102.0304.0506 detail
[...]
Local Roaming Client:
Client ACLs: xwf,fbs
Client State Servers: a03d.6f6b.bebe, cc16.7edc.27d8
```

Verifying Express Wi-Fi by Facebook Configurations on the AP

To view client state, use the following command:

```
Device# show flexconnect client
```

To view all ACLs applied to a specific client, use the following command:

Device# **show client access-list {post-auth | pre-auth} all** *client_mac_address*

```
Device# show client access-list post-auth all 1C:36:BB:10:1B:2C
Post-Auth URL ACLs for Client: 1C:36:BB:10:1B:2C IPv4 ACL: xwf
Fbs
IPv6 ACL:
ACTION  URL-LIST
allow cisco.com
allow yahoo.com
allow google.com
allow xwf.facebook.com
allow xwf-static.xx.fbcdn.net allow cisco-us.expresswifi.com allow xwf-scontent.xx.fbcdn.net
 allow xwfcisco-us.expresswifi.com
Resolved IPs for Client: 1C:36:BB:10:1B:2C HIT-COUNT URL ACTION IP-LIST
xwf
rule 0:
```

```
rule 1:
rule 2:
rule 3:
rule 4:
rule 5:
rule 6:
allow true and ip proto 6 and dst port 22
allow true and ip proto 6 and src port 22
allow true and dst 171.70.168.183 mask 255.255.255.255 allow true and src 171.70.168.183
mask 255.255.255.255 allow true and dst 157.240.22.50 mask 255.255.255.255 allow true and
src 157.240.22.50 mask 255.255.255.255 allow true and src 30.1.1.155 mask 255.255.255.255
and dst
30.1.1.18 mask 255.255.255.255 and ip proto 1
rule 7: allow true and src 30.1.1.18 mask 255.255.255.255 and dst
30.1.1.155 mask 255.255.255.255 and ip proto 1 rule 8: allow true and ip proto 17 rule 9:
allow true and ip proto 17 rule 10: deny all
fbs
rule 0: allow true and dst 31.13.0.0 mask 255.255.0.0
rule 1: allow true and dst 66.220.0.0 mask 255.255.0.0
rule 6: allow true and src 31.13.0.0 mask 255.255.0.0
rule 10: allow true and src 179.60.0.0 mask 255.255.0.0
rule 12: allow true and dst 171.70.168.183 mask 255.255.255.255 rule 14: allow true and ip
 proto 17
        rule 16: deny all
No IPv6 ACL found
```

```
Device# show client access-list pre-auth all 1C:36:BB:10:1B:2C
Pre-Auth URL ACLs for Client: 1C:36:BB:10:1B:2C
IPv4 ACL: xwf
IPv6 ACL:
ACTION  URL-LIST
allow cisco.com
allow yahoo.com
allow google.com
allow xwf.facebook.com
allow xwf-static.xx.fbcdn.net allow cisco-us.expresswifi.com allow xwf-scontent.xx.fbcdn.net
 allow xwfcisco-us.expresswifi.com
Resolved IPs for Client: 1C:36:BB:10:1B:2C HIT-COUNT URL ACTION IP-LIST
xwf
rule 0: allow true and ip proto 6 and dst port 22
rule 1: allow true and ip proto 6 and src port 22
rule 2: allow true and dst 171.70.168.183 mask 255.255.255.255 rule 3: allow true and src
171.70.168.183 mask 255.255.255.255 rule 4: allow true and dst 157.240.22.50 mask
255.255.255.255 rule 5: allow true and src 157.240.22.50 mask 255.255.255.255 rule 6: allow
 true and src 30.1.1.155 mask 255.255.255.255 and dst
30.1.1.18 mask 255.255.255.255 and ip proto 1
rule 7: allow true and src 30.1.1.18 mask 255.255.255.255 and dst
30.1.1.155 mask 255.255.255.255 and ip proto 1 rule 8: allow true and ip proto 17 rule 9:
allow true and ip proto 17 rule 10: deny all
No IPv6 ACL found
Redirect URL for client: 1C:36:BB:10:1B:2C
https://xwfcisco-us.expresswifi.com/customer/captive_portal
```

To view authentication server details applied to a specific client, use the following command where the **wlan_id** ranges from 1 to 15:

Device# **show running-config authentication dot11radio {0 | 1} wlan** *wlan_id*

```
Device# show running-config authentication dot11radio 1 wlan 1
bssid=00:a7:42:f6:4a:8e ssid=aa_namsoo_webauth beacon_period=100
auth=LOCAL AP_OPER_MODE=CONNECTED AP_OPER_MODE from WPA=CONNECTED
AUTH_SERVER[0]=30.1.1.18 AUTH_SERVER_PORT[0]=2812 ACCT_SERVER[0]=30.1.1.18
ACCT_SERVER_PORT[0]=2813 AUTH_SERVER[0]=30.1.1.18 AUTH_SERVER_PORT[0]=2812
ACCT_SERVER[0]=30.1.1.18 ACCT_SERVER_PORT[0]=2813
```

To view client accounting details, use the following command:

Device# **show controller dot11Radio** *{0|1}* **client** *client_mac_address*

```
Device# show client access-list pre-auth redirect-url 1C:36:BB:10:1B:2C
Redirect URL for client: 1C:36:BB:10:1B:2C
https://xwfcisco-us.expresswifi.com/customer/captive_portal
```

To view DCDS (distributed client datastore) or roaming configuration details for an associated client, use the following command:

Device# **show dot11 clients data-store details** *client_mac_address*

```
Device# show dot11 clients data-store details 1C:36:BB:10:1B:2C
First AP Name: APF8B7.E2CC.5D48
Current AP Name: APF8B7.E2CC.5D48
Current AP IP: 30.1.1.169
Current AP BSSID: f8:b7:e2:cd:cb:8e
Current AP SSID: aa_namsoo_webauth
Client VLAN: 1
Client State: 4
Audit Session ID: 3204365612
Accounting Session ID High: 0
Accounting Session ID Low: 0
Client Traffic Class Name: xwf
Client Traffic Class Name: fbs
```

CHAPTER 185

User Defined Network

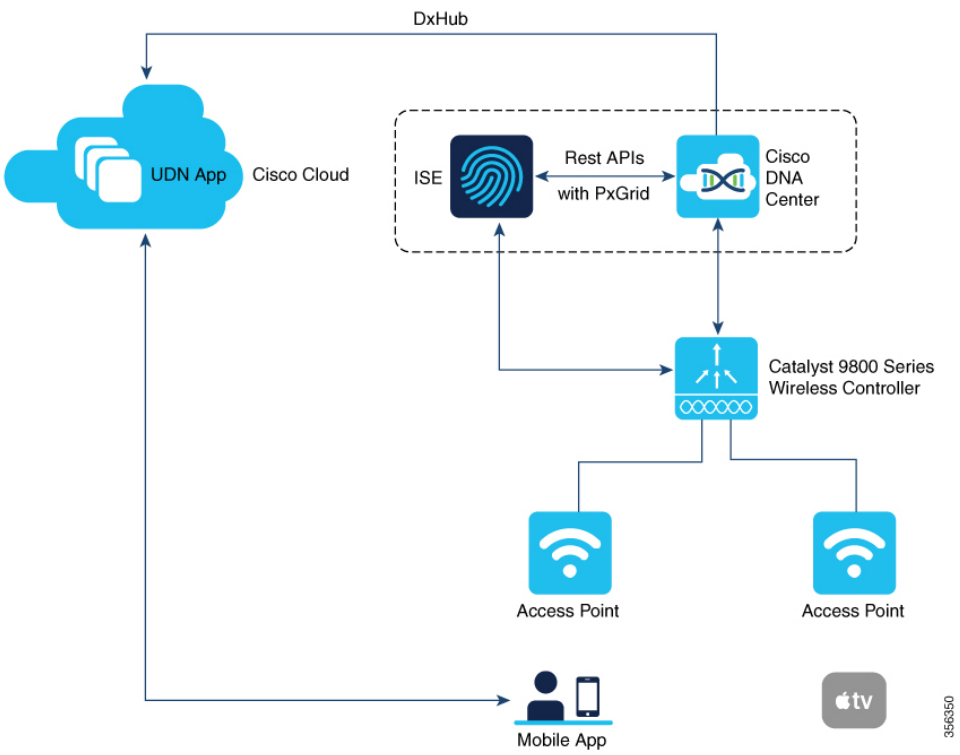
- Information About User Defined Network, on page 2077
- Restrictions for User Defined Network, on page 2079
- Configuring a User Defined Network, on page 2079
- Configuring a User Defined Network (GUI), on page 2081
- Verifying User Defined Network Configuration, on page 2081

Information About User Defined Network

A user defined network (UDN) is a solution that is aimed at providing secure and remote on-boarding of devices in shared service environments like dormitory rooms, resident halls, class rooms and auditoriums. This solution allows users to securely use Simple Discovery Protocols (SDP) like Apple Bonjour and mDNS-based protocols (Air Play, Air Print, Screen Cast, Print, and so on.), and UPnP based protocols to interact and share information with only their registered devices in a shared environment. It also enables the users to share their devices and resources with friends and roommates securely.

The UDN solution provides an easy way to create a virtual segment that allows user to create a private segment to add their devices. Traffic (unicast, non-Layer 3 multicast, or broadcast) to these devices can be seen only by other devices and users in the private segment. This feature also eliminates the security concern where users knowingly or unknowingly take control of devices that belong to other users in a shared environment. As of now, the UDN is supported only in local mode.

Figure 55: User Defined Network Topology



User Defined Network Solution Workflow

- User Defined Network is enabled on the controller, using policy profile, and the policy configuration is pushed to all the WLANs on a site.
- User Defined Network association is automatically generated by the UDN cloud service and is inherited by all the devices belonging to an user.
- Users can add or modify devices to the User Defined Network assigned to them by using a web portal or a mobile application. Users can also add devices to another User Defined Network, if they are invited to join that User Defined Network.
- The controller is updated with the client or resource information assigned to the User Defined Network.

Note Cisco Identity Services Engine (ISE) policy infrastructure is not used to update User Defined Network information. Whenever, there is a change in the User Defined Network, the ISE updates the controller with an explicit or a separate Change of Authorization (CoA) containing only the change of the User Defined Network ID.

Restrictions for User Defined Network

- A user can be associated to only one UDN.
- Roaming across controllers is not supported.
- This feature is not applicable for Cisco Mobility Express and Cisco AireOS platforms. Hence, IRCM is not supported.
- This feature is supported only in local mode on the Wave 2 access points and Cisco Catalyst 9100 series access points.
- This feature is supported only for centrally switched SSIDs.
- This feature is not supported for Flex mode APs.
- This feature is not supported for Fabric SSIDs.
- This feature is not supported for Guest Anchor scenario.
- Layer 2 and Layer 3 roaming is not supported.
- Layer 3 multicast (except SSDP/UPnP) containment using UDN is not supported, L3 multicast will continue to work as it is today.
- It is not recommended to enable user-defined **drop unicast** option in GUI if UDN is disabled.
- It is recommended to disable UDN from policy profile in SSIDs when integrating UDN+ solution with Cisco exclusive partner Splash Access.

Note The UDN+ simplifies the solution and brings the same unique user experience for both Meraki and Cisco Catalyst 9800 Series Wireless Controller based deployments.

Configuring a User Defined Network

The User Defined Network configuration is site based and is added as part of a policy profile. When applied, the policy is enforced to all the clients or devices in a network for a site, across WLANs.

When enabled, the policy profile also enforces the filtering of mDNS queries based on the UDN-ID.

Before you begin

- RADIUS server should be configured for the UDN solution to work.
- Configure aaa-override in the policy profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy policy-wpn`	Creates a policy profile. *profile-name* is the profile name of the policy profile.
Step 3	**user-defined-network** **Example:** `Device(config-wireless-policy)# user-defined-network`	Enables user defined private-network.
Step 4	**user-defined-network drop-unicast** **Example:** `Device(config-wireless-policy)# user-defined-network drop-unicast`	Sets action to drop unicast traffic. By default, unicast traffic is allowed across UDN.
Step 5	**exit** **Example:** `Device(config-wireless-policy)# exit`	Enters global configuration mode.
Step 6	**ap remote-lan-policy policy-name** *policy-name* **Example:** `Device(config)# ap remote-lan-policy policy-name policy-wpn`	Configures a remote LAN policy profile.
Step 7	**user-defined-network** **Example:** `Device(config-remote-lan-policy)# user-defined-network`	Enables user defined private-network.
Step 8	**user-defined-network drop-unicast** **Example:** `Device(config-remote-lan-policy)# user-defined-network drop-unicast`	Sets action to drop unicast traffic.

Configuring a User Defined Network (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Policy**.

Step 2 In the **Policy Profile** window, select a policy profile.

Step 3 In the **Edit Policy Profile** window, click the **Advanced** tab.

Step 4 In the **User Defined Network** section, check the **Status** check box to enable a user personal network.

Step 5 Check the **Drop Unicast** check box to set the action to Drop Unicast traffic.

By default, unicast traffic is not contained.

Verifying User Defined Network Configuration

To view the status of the UDN feature (either enabled or disabled) and also information about the drop unicast flag, use the following command:

```
Device# show wireless profile policy detailed default-policy-profile

User Defined (Private) Network               : Enabled
User Defined (Private) Network Unicast Drop  : Enabled
```

To view the name of the UDN to which the client belongs, use the following command:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 detailed

User Defined (Private) Network : Enabled
User Defined (Private) Network Drop Unicast : Enabled
              Private group name: upn*group*7
              Private group id : 7777
              Private group owner: 1
              Private group name: upn*group*7
              Private group id : 7777
              Private group owner:
```

To view the UDN payload sent from an AP to the controller, use the following command:

```
Device# show wireless stats client detail | inc udn

Total udn payloads sent                          : 1
```

When mDNS gateway is enabled on the controller, the mDNS services are automatically filtered based on the user private network ID for all the clients on the WLANs where user private network is enabled.

To view the service instances of a private network, use the following command:

```
Device# show mdns-sd cache udn 7777 detail

Name: _services._dns-sd._udp.local
  Type: PTR
  TTL: 4500
  WLAN: 2
```

```
  WLAN Name: mdns-psk
  VLAN: 16
  Client MAC: f4f9.51e2.a6a6
  AP Ethernet MAC: 002a.1087.d68a
  Remaining-Time: 4486
  Site-Tag: default-site-tag
  mDNS Service Policy: madhu-mDNS-Policy
  Overriding mDNS Service Policy: NO
  UDN-ID: 7777
  UDN-Status: Enabled
  Rdata: _airplay._tcp.local
.
.
.
```

To view the service instances that are learnt from a shared UDN ID, use the following command:

```
Device# show mdns-sd cache udn shared

------------------------------------------------------------- PTR Records
-----------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
-------------------------------------------------------------------------------------------------------------------
9.1.1.7.5.D.E.F.F.F.6.C.7.E.2.1.0.0.0.0.0.0.0  4500     WLAN      2     10e7.c6d5.7119
HP10E7C6D57119-2860.local
_services._dns-sd._udp.local                   4500     WLAN      2     10e7.c6d5.7119
_ipps._tcp.local
_universal._sub._ipps._tcp.local               4500     WLAN      2     10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_print._sub._ipps._tcp.local                   4500     WLAN      2     10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_ePCL._sub._ipps._tcp.local                    4500     WLAN      2     10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_ipps._tcp.local                               4500     WLAN      2     10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_services._dns-sd._udp.local                   4500     WLAN      2     10e7.c6d5.7119
_ipp._tcp.local
_universal._sub._ipp._tcp.local                4500     WLAN      2     10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_print._sub._ipp._tcp.local                    4500     WLAN      2     10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_ePCL._sub._ipp._tcp.local                     4500     WLAN      2     10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_ipp._tcp.local                                4500     WLAN      2     10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
.
.
.

------------------------------------------------------------- SRV Records
-----------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
-------------------------------------------------------------------------------------------------------------------
HP DeskJet 5000 series [D57119] (3127)._ipp._  4500     WLAN      2     10e7.c6d5.7119   0
 0 631 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._http.  4500     WLAN      2     10e7.c6d5.7119   0
 0 80 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._ipps.  4500     WLAN      2     10e7.c6d5.7119   0
 0 631 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._uscan  4500     WLAN      2     10e7.c6d5.7119   0
 0 8080 HP10E7C6D57119-2860.local
.
.
```

```
.
------------------------------------------------------------ A/AAAA Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
-------------------------------------------------------------------------------------------------------------------
HP10E7C6D57119-2860.local                      4500     WLAN      2     10e7.c6d5.7119
8.16.16.99

------------------------------------------------------------ TXT Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
-------------------------------------------------------------------------------------------------------------------
HP DeskJet 5000 series [D57119] (3127)._ipp._  4500     WLAN      2     10e7.c6d5.7119
[502]'txtvers=1''adminurl=http://HP10E7C6D57119-28
HP DeskJet 5000 series [D57119] (3127)._http.  4500     WLAN      2     10e7.c6d5.7119
[1]''
HP DeskJet 5000 series [D57119] (3127)._ipps.  4500     WLAN      2     10e7.c6d5.7119
[502]'txtvers=1''adminurl=http://HP10E7C6D57119-28
.
.
.
```

To view the multicast DNS (mDNS) Service Discovery cache detail, use the following command:

```
Device# show mdns-sd cache detail

Name: _printer._tcp.local
  Type: PTR
  TTL: 4500
  VLAN: 21
  Client MAC: ace2.d3bc.047e
  Remaining-Time: 4383
  mDNS Service Policy: default-mdns-service-policy
  Rdata: HP OfficeJet Pro 8720 [BC047E] (2)._printer._tcp.local
```

CHAPTER 186

Hotspot 2.0

- Introduction to Hotspot 2.0, on page 2085
- Open Roaming, on page 2087
- Configuring Hotspot 2.0, on page 2089

Introduction to Hotspot 2.0

The Hotspot 2.0 feature enables IEEE 802.11 devices to interwork with external networks. The interworking service aids network discovery and selection, enabling information transfer from external networks. It provides information to the stations about the networks before association.

Interworking not only helps users within the home, enterprise, and public access domains, but also assists manufacturers and operators to provide common components and services for IEEE 802.11 customers. These services are configured on a per-WLAN basis on the Cisco Wireless Controller (controller).

Hotspot 2.0, also known as HS2 and Wi-Fi Certified Passpoint, is based on the IEEE 802.11u and Wi-Fi Alliance Hotspot 2.0 standards. It seeks to provide better bandwidth and services-on-demand to end users. The Hotspot 2.0 feature allows mobile devices to join a Wi-Fi network automatically, including during roaming, when the devices enter the Hotspot 2.0 area.

The Hotspot 2.0 feature has four distinct parts:

- Hotspot 2.0 Beacon Advertisement: Allows a mobile device to discover Hotspot 2.0-compatible and 802.11u-compatible WLANs.
- Access Network Query Protocol (ANQP) Queries: Sends queries about the networks from IEEE 802.11 devices, such as network type (private or public); connectivity type (local network, internet connection, and so on), or the network providers supported by a given network.
- Online Sign-up: Allows a mobile device to obtain credentials to authenticate itself with the Hotspot 2.0 or WLAN.
- Authentication and Session Management: Provides authentication (802.1x) and management of the STA session (session expiration, extension, and so on).

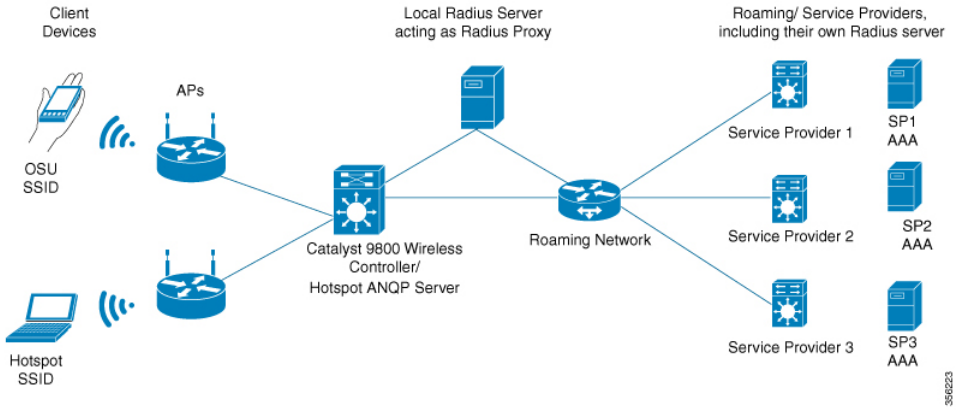
In order to mark a WLAN as Hotspot 2.0-compatible, the 802.11u-mandated information element and the Hotspot 2.0 information element is added to the basic service set (BSS) beacon advertised by the corresponding AP, and in WLAN probe responses.

Note The Hotspot 2.0 feature supports only local mode or FlexConnect mode (central switching and central authentication).

FlexConnect local switching is only supported when the Open Roaming configuration template is set up using the **wireless hotspot anqp-server** *server-name* **type open-roaming** command. If the configuration diverges from this template, FlexConnect local switching will not be supported.

The following figure shows a standard deployment of the Hotspot 2.0 network architecture:

Figure 56: Hotspot 2.0 Deployment Topology



Hotspot 2.0 Enhancements

From Cisco IOS XE Amsterdam 17.3.1, the Hotspot 2.0 feature has been enhanced with the following options:

- New ANQP elements:
  - Advice of charge: Provides information on the financial charges for using the SSID of the NAI realm
  - Operator icon metadata
  - Venue URL: Defines an optional URL for each of the configured venue names
- Introduction of Terms and Conditions: This requires a user to accept certain Terms and Conditions before being allowed internet access, after connecting to a Hotspot SSID.
- Integration of OSEN security and WPA2 security on the same SSID.

From Cisco IOS XE Amsterdam 17.3.1 onwards, two encryption methods are supported on a single SSID, namely WPA2 802.1x for Hotspot 2.0 and OSEN for online sign-up. Based on the type of encryption selected during client association, the client will be put on Hotspot 2.0 VLAN or online sign-up VLAN.

In WPA2 802.1x authentication, a client should match the credentials provisioned on a device. In online sign-up, a service provider WLAN is used by a client to perform online sign-up. For Hotspot 2.0 SSIDs, the RADIUS server enforces the terms and conditions before allowing internet connectivity to clients.

This release also supports OSEN-specific VLAN in a policy profile. If an OSEN VLAN is defined in a policy profile, OSEN clients are added to the VLAN. Otherwise, clients are added to the regular policy profile VLAN

or to the default VLAN. If OSEN is enabled with WPA2 on an SSID, it is mandatory to define an OSEN VLAN in the policy profile. Otherwise, clients cannot join the VLAN.

In FlexConnect mode, if an OSEN VLAN is defined in a policy profile, the same VLAN needs to be added to the flex profile. Failing to do so excludes the clients from the VLAN.

Note When Hotspot 2.0 is enabled in a WLAN, the Wi-Fi direct clients that support cross-connect feature should not be allowed to associate to the Hotspot 2.0 WLAN. To make sure this policy is enforced, ensure that the following configuration is in place:

```
wlan <wlan-name> <wlan-name> <ssid>
wifi-direct policy xconnect-not-allow
```

Restrictions

- Clients are excluded if an OSEN VLAN is not added to a flex profile.
- In FlexConnect mode, clients are excluded if an OSEN VLAN is not added in a flex profile.
- In FlexConnect deployments, the URL filter should reference an existing URL filter (configured using the **urlfilter list** *urlfilter-name* command). Otherwise, a client is added to the excluded list, after authentication.
- Only central authentication is supported.
- Fragmented ANQP replies are not synchronized to the standby controller in high-availability mode. Therefore, clients have to re-issue a query if there is a switchover.

Open Roaming

From Cisco IOS XE Amsterdam Release 17.2.1, the controller supports open roaming configuration, which enables mobile users to automatically and seamlessly roam across Wi-Fi and cellular networks.

The new configuration template of the open roaming ANQP server simplifies the task of setting up a Hotspot 2.0 ANQP server. When you configure open roaming, fixed ANQP parameters are automatically populated.

You can configure different identity types by defining roaming organizational identifiers. The organizational unique identifier (OUI) is a three-octet number that identifies the type of organizations available in a given roaming consortium. The OUI list determines the type of identities allowed to roam into the network. The default configuration allows all the identities on the access network. However, access networks can customize the Roaming Consortium Organization Identifier (RCOI) they advertise.

You can configure three types of policies for access networks:

- Allow all: Accepts users from any identity provider (IDP), with any privacy policy.
- Real ID: Accepts users from any IDP, but only with a privacy policy that shares real identity (anonymous not accepted).
- Custom: Accepts users of select identity types and privacy policies associated with the identity types; basically all the other RCOIs.

Users can select the following privacy modes:

- Anonymous
- Share real identity

The list of currently defined organizational identifiers and their aliases are given in the following table.

Table 143: Roaming Organizational Identifiers and Aliases

Description	Roaming Organizational Identifier	WBA Value	Display Name
All	004096	5A03BA0000	All
All with real ID	00500b	5A03BA1000	All with real-id only
All paid members	00500f	BAA2D00000	All paid
Device manufacturer all ID	00502a	5A03BA0A00	Device Manufacturer
Device manufacturer real ID only	0050a7	5A03BA1A00	Device Manufacturer real-id
Cloud or Social ID	005014	5A03BA0200	Cloud ID
Cloud or Social real ID	0050bd	5A03BA1200	Cloud ID real-id
Enterprise Employee ID	00503e	5A03BA0300	Enterprise ID
Enterprise Employee real ID	0050d1	5A03BA1300	Enterprise ID real ID
Enterprise Customer ID	005050	-	Enterprise Customer program ID
Enterprise Customer real ID	0050e2	-	Enterprise Customer program real ID
Loyalty Retail ID	005053	5A03BA0B00	Loyalty Retail
Loyalty Retail real ID	0050f0	5A03BA1B00	Loyalty Retail real ID
Loyalty Hospitality ID	005054	5A03BA0600	Loyalty Hospitality
Loyalty Hospitality real ID	00562b	5A03BA1600	Loyalty Hospitality real ID
SP free Bronze Qos	005073	5A03BA0100	SP free Bronze Qos
SP free Bronze Qos Real ID	0057D2	5A03BA1100	SP free Bronze Qos Real ID
SP paid Bronze QoS	-	BAA2D00100	SP paid Bronze QoS
SP paid Bronze QoS real ID	-	BAA2D01100	SP paid Bronze QoS real ID
SP paid Silver QoS	-	BAA2D02100	SP paid Silver QoS
SP paid Silver QoS real ID	-	BAA2D03100	SP paid Silver QoS real ID
SP paid Gold QoS	-	BAA2D04100	SP paid Gold QoS

Description	Roaming Organizational Identifier	WBA Value	Display Name
SP paid Gold QoS real ID	-	BAA2D05100	SP paid Gold QoS real ID
Government ID free	-	5A03BA0400	Government ID free
Automotive ID free	-	5A03BA0500	Automotive ID free
Automotive Paid	-	BAA2D00500	Automotive Paid
Education or Research ID free	-	5A03BA0800	Education or Research ID free
Cable ID free	-	5A03BA0900	Cable ID free

Configuring Hotspot 2.0

Configuring an Access Network Query Protocol Server

The Access Network Query Protocol Server (ANQP) is a query and response protocol that defines the services offered by an AP, usually at a Wi-Fi Hotspot 2.0.

Note When configuring roaming-oi in the ANQP server, ensure that you set the **beacon** keyword for at least one roaming-oi, as mandated by the 802.11u standard.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless hotspot anqp-server** *server-name* **Example:** `Device(config)# wireless hotspot anqp-server my_server`	Configures a Hotspot 2.0 ANQP server.
Step 3	**description** *description* **Example:** `Device(config-wireless-anqp-server)# description "My Hotspot 2.0"`	Adds a description for the ANQP server.
Step 4	**3gpp-info** *mobile-country-code mobile-network-code*	Configures a 802.11u Third Generation Partnership Project (3GPP) cellular network.

	Command or Action	Purpose
	Example: `Device(config-wireless-anqp-server)# 3gpp-info us mcc`	The *mobile-country-code* should be a 3-digit decimal number. The *mobile-network-code* should be a 2-digit or 3-digit decimal number.
Step 5	**anqp fragmentation-threshold** *threshold-value* **Example:** `Device(config-wireless-anqp-server)# anqp fragmentation-threshold 100`	Configures the ANQP reply fragmentation threshold, in bytes. The ANQP protocol can be customized by setting the fragmentation threshold, after which the ANQP reply is split into multiple messages. **Note** We recommend that you use the default values for the deployment.
Step 6	**anqp-domain-id** *domain-id* **Example:** `Device(config-wireless-anqp-server)# anqp-domain-id 100`	Configures the Hotspot 2.0 ANQP domain identifier.
Step 7	**authentication-type** {**dns-redirect** | **http-https-redirect** | **online-enrollment** | **terms-and-conditions**} **Example:** `Device(config-wireless-anqp-server)# authentication-type online-enrollment`	Configures the 802.11u network authentication type. Depending on the authentication type, a URL is needed for HTTP and HTTPS.
Step 8	**connection-capability** *ip-protocol port-number* {**closed** | **open** | **unknown**} **Example:** `Device(config-wireless-anqp-server)# connection-capability 12 40 open`	Configures the Hotspot 2.0 protocol and port capabilities. **Note** Hotspot 2.0 specifications require that you predefine some open ports and protocols. Ensure that you meet these requirements in order to comply with the Hotspot 2.0 specifications. See the **connection-capability** command in the Cisco Catalyst 9800 Series Wireless Controller Command Reference document for a list of open ports and protocols.
Step 9	**domain** *domain-name* **Example:** `Device(config-wireless-anqp-server)# domain my-domain`	Configures an 802.11u domain name. You can configure up to 32 domain names. The *domain-name* should not exceed 220 characters.
Step 10	**ipv4-address-type** *ipv4-address-type* **Example:**	Configures an 802.11u IPv4 address type in the Hotspot 2.0 network.

	Command or Action	Purpose
	`Device(config-wireless-anqp-server)# ipv4-address-type public`	
Step 11	**ipv6-address-type** *ipv6-address-type* **Example:** `Device(config-wireless-anqp-server)# ipv6-address-type available`	Configures an 802.11u IPv6 address type in the Hotspot 2.0 network.
Step 12	**nai-realm** *realm-name* **Example:** `Device(config-wireless-anqp-server)# nai cisco.com`	Configures an 802.11u NAI realm profile that identifies the realm that is accessible using the AP.
Step 13	**operating-class** *class-id* **Example:** `Device(config-wireless-anqp-server)# operating-class 25`	Configures a Hotspot 2.0-operating class identifier.
Step 14	**operator** *operator-name language-code* **Example:** `Device(config-wireless-anqp-server)# operator XYZ-operator eng`	Configures a Hotspot 2.0 operator-friendly name in a given language. Use only the first three letters of the language, in lower case, for the language code. For example, use *eng* for English. To see the full list of language codes, go to: http://www.loc.gov/standards/iso639-2/php/code_list.php. **Note** You can configure only one operator per language.
Step 15	**osu-ssid** *SSID* **Example:** `Device(config-wireless-anqp-server)# osu-ssid test`	Configures the SSID that wireless clients will use for OSU. The SSID length can be up to 32 characters.
Step 16	**roaming-oi** *OI-value* [**beacon**] **Example:** `Device(config-wireless-anqp-server)# roaming-oi 24 beacon`	Configures the 802.11u roaming organization identifier. If the **beacon** keyword is specified, the roaming OUI is advertised in the AP WLAN beacon or probe response. Otherwise, it will only be returned while performing the roaming OUI ANQP query. **Note** The hex string of a roaming OUI should contain only lowercase letters.
Step 17	**venue** *venue-name language-code*	Configures the 802.11u venue information.

	Command or Action	Purpose
	Example: `Device(config-wireless-anqp-server)# venue bank eng`	The *venue-name* should not exceed 220 characters and the *language-code* should only be 2 or 3 lowercase letters (a-z) in length.

Configuring ANQP Global Server Settings (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Hotspot/OpenRoaming**.

Step 2 Select an existing server from the list of servers.

Step 3 Click the **Server Settings** tab.

Step 4 Go to the **Global Server Settings** section.

Step 5 From the **IPv4 Type** drop-down list, choose an IPv4 type.

Step 6 From the **IPv6 Type** drop-down list, choose an IPv6 type.

Step 7 In the **OSU SSID** field, enter the SSID that wireless clients will use for Online Sign-Up (OSU).

Step 8 Click the **Show Advanced Configuration** link to view the advanced options.

- In the **Fragmentation Threshold (bytes)** field, enter the fragmentation threshold.

  Note Packets that are larger than the size you specify here will be fragmented.

- In the **GAS Request Timeout (ms)** field, enter the number of Generic Advertisement Services (GAS) request action frames sent that can be sent to the controller by an AP in a given interval.

Step 9 Click **Apply to Device**.

Configuring Open Roaming (CLI)

The new configuration template of the open roaming ANQP server simplifies the task of setting up a Hotspot 2.0 ANQP server. When you configure open roaming using this template, default ANQP parameters are automatically populated. The default values defined in the template always override any user-defined configuration values. For example, these are the default values enforced with the type open-roaming template:

- nai-realm open.openroaming.org
- eap-method eap-tls
- eap-method eap-ttls
- inner-auth-non-eap mschap-v2
- inner-auth-non-eap pap
- eap-method eap-aka

You can add more fields to the existing template, but ensure that they do not overlap with the existing default values. Also, if you change any of these default values, you will need to re-configure every time you enter in anqp type open-roaming config.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless hotspot anqp-server** *server-name* **type open-roaming** **Example:** `Device(config)# wireless hotspot anqp-server my-server type open-roaming`	Configures a Hotspot 2.0 ANQP server with open roaming.
Step 3	**open-roaming-oi** *alias* **Example:** `Device(config-wireless-anqp-server)# open-roaming-oi allow-all`	Sets the open roaming element alias.
Step 4	**domain** *domain-name* **Example:** `Device(config)# domain my-domain`	Configures a preferred domain name to ensure that clients roam into a preferred network. You can configure up to 32 domain names. The *domain-name* should not exceed 220 characters.

Configuring Open Roaming (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Hotspot/OpenRoaming**.

Step 2 Click **Add**.

The **Add New ANQP Server** window is displayed.

Step 3 In the **Name** field, enter a name for the server.

Step 4 In the **Description** field, enter a description for the server.

Step 5 Check the **OpenRoaming Server** check box to use the server as an open roaming server.

Note You can set the server as an open roaming server only at the time of server creation.

Step 6 Check the **Internet Access** check box to enable internet access for the server.

Step 7 From the **Network Type** drop-down list, choose the network type.

Step 8 Click **Apply to Device**.

Configuring NAI Realms (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Hotspot/OpenRoaming**.

Step 2 Select an existing server from the list of servers.

Step 3 Go to the **NAI Realms** section.

Step 4 Click **Add**.

The **Add NAI Realm** window is displayed.

Step 5 In the **NAI Realm Name** field, enter an 802.11u NAI realm of the OSU operator.

Step 6 In the **EAP Methods** section, use the toggle button to enable the required EAP methods.

After an EAP method is enabled, a pane is displayed to configure the details. Users are shown a configuration section where they can enable *credential*, *inner-auth-eap*, *inner-auth-non-eap*, *tunneled-eap-credential*. The user can select multiple options for each of the configuration.

- The **Credential** window has options such as certificate, hw-token, nfc, none, sim, softoken, username-password, and usim. Check the corresponding check box.
- The **inner-auth-eap** window has options such as eap-aka, eap-fast, eap-sim, eap-tls, eap-ttls, eap-leap, and eap-peap. Check the corresponding check box.
- The **inner-auth-eap** window has options such as eap-aka, eap-fast, eap-sim, eap-tls, eap-ttls, eap-leap, and eap-peap. Check the corresponding check box.
- The **tunneled-eap-credential** window has options such as anonymous, certificate, hw-token, nfc, sim, softoken, username-password, and usim. Check the corresponding check box.
- Click **Save**.

Step 7 Click **Apply to Device**.

Configuring Organizational Identifier Alias (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Hotspot/OpenRoaming**.

Step 2 Select an existing server from the list of servers.

Step 3 In the **Roaming OIs** area, enter an 802.11u roaming organization identifier in the **Roaming OI** field.

Step 4 Check the **Beacon State** check box to enable the beacon.

If the beacon is specified, the roaming OUI is advertised in the AP WLAN beacon or probe response. Otherwise, it will only be returned while performing the roaming OUI ANQP query.

Note Only three OUIs can be enabled in the beacon state.

Step 5 Click **Add** to add a roaming OI.

Step 6 In the **Available OpenRoaming OI** window, a list of organizational identifiers are displayed, along with the ones you have added. Select an organizational identifier and click the right arrow to add an **OpenRoaming OI**.

Step 7 In the **Domains** area, enter an 802.11u domain name in the **Domain Name** field.

Step 8 Click **Add** to use the domain name that you have entered as the preferred domain.

Step 9 Click **Apply to Device**.

Configuring WAN Metrics (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Hotspot/OpenRoaming**.

Step 2 Select an existing server from the list of servers.

Step 3 Click the **Server Settings** tab.

Step 4 Go to the **WAN Metrics** area.

Step 5 In the **Downlink Load** field, enter the WAN downlink load.

Step 6 In the **Downlink Speed (kbps)** field, enter the WAN downlink speed, in kbps.

Step 7 In the **Load Duration (100ms)** field, enter the load duration.

Step 8 In the **Upload Load** field, enter the WAN upload load.

Step 9 In the **Upload Speed (kbps)** field, enter the WAN upload speed, in kbps.

Step 10 From the **Link Status** drop-down list, choose the link status.

Step 11 Use the **Full Capacity Link** toggle button to enable the WAN link to operate at its maximum capacity.

Step 12 Click **Apply to Device**.

Configuring WAN Metrics

This procedure shows you how to configure the Wide Area Network (WAN) parameters such as uplink and downlink speed, link status, load, and so on.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless hotspot anqp-server** *server-name* **Example:**	Configures a Hotspot 2.0 ANQP server.

	Command or Action	Purpose
	`Device(config)# wireless hotspot anqp-server my_server`	
Step 3	**wan-metrics downlink-load** *load-value* **Example:** `Device(config-wireless-anqp-server)# wan-metrics downlink-load 100`	Configures the WAN downlink load.
Step 4	**wan-metrics downlink-speed** *speed* **Example:** `Device(config-wireless-anqp-server)# wan-metrics downlink-speed 1000`	Configures the WAN downlink speed, in kbps.
Step 5	**wan-metrics full-capacity-link** **Example:** `Device(config-wireless-anqp-server)# wan-metrics full-capacity-link`	Configures the WAN link to operate at its maximum capacity.
Step 6	**wan-metrics link-status** {**down** | **not-configured** | **test-state** | **up**} **Example:** `Device(config-wireless-anqp-server)# wan-metrics link-status down`	Sets the WAN link status.
Step 7	**wan-metrics load-measurement-duration** *duration* **Example:** `Device(config-wireless-anqp-server)# wan-metrics load-measurement-duration 100`	Configures the uplink or downlink load measurement duration.
Step 8	**wan-metrics uplink-load** *load-value* **Example:** `Device(config-wireless-anqp-server)# wan-metrics uplink-load 100`	Configures the WAN uplink load.
Step 9	**wan-metrics uplink-speed** *speed* **Example:** `Device(config-wireless-anqp-server)# wan-metrics uplink-speed 1000`	Configures the WAN uplink speed, in kbps.

Configuring Beacon Parameters (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Hotspot/OpenRoaming**.

Step 2 Select an existing server from the list of servers.

Step 3 Click **Server Settings** tab.

Step 4 Go to the **Beacon Parameters** section.

Step 5 In the **Hess id** field, enter the homogenous extended service set identifier. The Hess ID can be either in *xx:xx:xx:xx:xx:xx*, *xx-xx-xx-xx-xx-xx*, or *xxxx.xxxx.xxxx* format.

Step 6 In the **Domain id** field, enter the domain's identifier.

Step 7 From the **Venue Type** drop-down list, select the venue.

Choosing a venue activates the subvenue type.

Step 8 From the **subvenue-type** drop-down list, select the sub-venue.

Step 9 Click **Apply to Device**.

Configuring Authentication and Venue (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Hotspot/OpenRoaming**.

Step 2 Select an existing server from the list of servers.

Step 3 Click the **Authentication/Venue** tab.

Step 4 Under the **Network Auth Types** section, check the **DNS Redirect**, **Online Enrolment**, **HTTP/HTTPS Redirect**, **Terms and Conditions** check boxes.

For **HTTP/HTTPS Redirect** and **Terms and Conditions**, the URL field is enabled after selecting them.

Step 5 Add the URL for the corresponding authentication type.

Step 6 Click **Apply**.

Step 7 Go to the **Venues** section and click **Add**.

The **Venue Details** pane is displayed.

Step 8 In the **Language Code** field, enter the language code.

Use the first two or three letters of the language, in lower case, for the language code. For example, use *eng* for English. To see the full list of language codes, go to: http://www.loc.gov/standards/iso639-2/php/code_list.php.

Step 9 In the **Venue URL** field, enter the URL of the venue.

Step 10 In the **Venue Name** field, enter the name of the venue.

Step 11 Click check mark icon to add the venue details.

Step 12 Go to the **Connection Capability** section and click **Add**.

The **Connection Capabilities** pane is displayed. See the **connection-capability** command in the Cisco Catalyst 9800 Series Wireless Controller Command Reference document for a list of open ports and protocols.

Step 13 In the **Port Number** field, enter the port number.

Step 14 From the **Connection Status** drop-down list, choose a connection status.

Step 15 In the **IP Protocol** field, enter the IP protocol number.

Hotspot 2.0 specifications require that you predefine some open ports and protocols. Ensure that you meet these requirements in order to comply with the Hotspot 2.0 specifications. See the **connection-capability** command in the Cisco Catalyst 9800 Series Wireless Controller Command Reference document for a list of open ports and protocols.

Step 16 Click the check mark icon to add the connection details.

Step 17 Click **Apply to Device**.

Configuring 3GPP/Operator (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Hotspot/OpenRoaming**.

Step 2 Select an existing server from the list of servers.

Step 3 Go to the **3GPP/Operator** tab.

Step 4 In the **Operating Class Indicator** field, enter the operating class identifier and click the + icon.

The operating class identifier is added and displayed in the pane below. Use the delete icon to delete them, if required.

Note Class IDs should be in the following ranges: 81-87, 94-96, 101-130, 180, and 192-254.

Step 5 Go to the **3GPP Cellular Networks** section and click **Add**.

The **3GPP Network Details** pane is displayed.

Step 6 In the **Mobile Country Code (MCC)** field, enter the mobile country code, which should be a 3-digit decimal number.

Step 7 In the **Mobile Network Code (MNC)** field, enter the mobile network code, which should be a 2 or 3-digit decimal number.

For the list of Mobile Country Codes (MCC) and Mobile Network Codes (MNC), see the following links: https://www.itu.int/pub/T-SP-E.212B-2018 or https://www.mcc-mnc.com.

Step 8 Click check mark icon to add the network details.

Step 9 Go to the **Hotspot 2.0 Operators** section and click **Add**.

The **Operator Details** pane is displayed.

Step 10 In the **Language Code** field, enter the language code.

Use only the first three letters of the language, in lower case, for the language code. For example, use *eng* for English. To see the full list of language codes, go to: http://www.loc.gov/standards/iso639-2/php/code_list.php.

Step 11 In the **Name** field, enter the name of the OSU operator.

Step 12 Click check mark icon to add the operator details.

Step 13 Click **Apply to Device**.

Configuring OSU Provider (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Hotspot/OpenRoaming**.

Step 2 Select an existing server from the list of servers.

Step 3 Go to the **OSU Provider** tab.

Step 4 Click **Add**.

The **General Config** pane is displayed.

Step 5 In the **Provider Name** field, enter the OSU provider name.

Step 6 In the **NAI Realm** field, enter the Network Access Identifier (NAI) realm of the OSU operator.

Step 7 From the **Primary Method** drop-down list, choose the primary supported OSU method of the OSU operator.

This activates the **Secondary Method** drop-down list. If you choose *None* as the primary supported OSU method, you will not get the secondary method.

Step 8 (Optional) From the **Secondary Method** drop-down list, choose the secondary supported OSU method of the OSU operator.

Step 9 In the **Server URI** field, enter the server Uniform Resource Identifier (URI) of the OSU operator.

Step 10 Click **Icon Config** tab.

Step 11 Click **Add**.

Step 12 From the **Icon Name** drop-down list, choose the icon name.

Step 13 Click **Save**.

Step 14 Click **Friendly Names** tab.

Step 15 Click **Add**.

Step 16 In the **Language** field, enter the language code.

Step 17 In the **Name** field, enter the name of the OSU operator.

Step 18 In the **Description** field, enter the description for the OSU operator.

Step 19 Click **Save**.

Step 20 Click the check mark icon to save.

Step 21 Click **Apply to Device**.

Configuring an Online Sign-Up Provider

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless hotspot icon bootflash:***system-file-name media-type language-code icon-width icon-height* **Example:** `Device(config)# wireless hotspot icon bootflash:logo1 image eng 100 200`	Configures an icon for Hotspot 2.0 and its parameters, such as media type, language code, icon width, and icon height.
Step 3	**wireless hotspot anqp-server** *server-name* **Example:** `Device(config)# wireless hotspot anqp-server my_server`	Configures a Hotspot 2.0 ANQP server.
Step 4	**osu-provider** *osu-provider-name* **Example:** `Device(config-wireless-anqp-server)# osu-provider my-osu`	Configures a Hotspot 2.0 OSU provider name.

Step 5	**name** *osu-operator-name lang-code description*
	Example:
	`Device(config-anqp-osu-provider)# name xyz-oper`
	`eng xyz-operator`
		Configures the name of the OSU operator in a given language.
		The *osu-operator-name* and *description* should not exceed 220 characters. The language code should be 2 or 3 lower-case letters (a-z).

Step 6	**server-uri** *server-uri* **Example:** `Device(config-anqp-osu-provider)# server-uri cisco.com`	Configures the server Uniform Resource Identifier (URI) of the OSU operator.
Step 7	**method** {**oma-dm** | **soap-xml-spp**} **Example:** `Device(config-anqp-osu-provider)# method oma-dm`	Configures the primary supported OSU method of the OSU operator.
Step 8	**nai-realm** *nai-realm* **Example:** `Device(config-anqp-osu-provider)# nai-realm cisco.com`	Configures the Network Access Identifier (NAI) realm of the OSU operator. The *nai-realm* should not exceed 220 characters.
Step 9	**icon** *file-name*	Configures the icon for the OSU provider.

	Command or Action	Purpose
	Example: `Device(config-anqp-osu-provider)# icon xyz.jpeg`	The *file-name* should not exceed 100 characters.

Configuring Hotspot 2.0 WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan hs2 1 hs2`	Configures a WLAN and enters WLAN configuration mode.
Step 3	**security wpa wpa2 gtk-randomize** **Example:** `Device(config-wlan)# security wpa wpa2 gtk-randomize`	Configures random GTK for hole 196 mitigation. Hole 196 is the name of WPA2 vulnerability.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring an Online Subscription with Encryption WLAN

Online subscription with Encryption (OSEN) WLAN is used to onboard a Hotspot 2.0 network (to get the necessary credentials) in a secure manner.

Note You cannot apply a policy profile to the OSEN WLAN if a Hotspot 2.0 server is enabled on the WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan hs2 1 hs2`	Configures a WLAN and enters WLAN configuration mode.
Step 3	**security wpa osen** **Example:** `Device(config-wlan)# security wpa osen`	Enables WPA OSEN security support. **Note** OSEN and robust security network (RSN) are mutually exclusive. If RSN is enabled on a WLAN, OSEN cannot be enabled on the same WLAN.
Step 4	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Attaching an ANQP Server to a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name ssid* **Example:** `Device(config)# wireless profile policy policy-hotspot`	Configures a policy profile.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the policy profile.
Step 4	**hotspot anqp-server** *server-name* **Example:** `Device(config-wireless-policy)# hotspot anqp-server my-server`	Attaches the Hotspot 2.0 ANQP server to the policy profile.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.

What to do next

Attach the policy profile to the WLAN to make the WLAN Hotspot 2.0 enabled.

Configuring Interworking for Hotspot 2.0

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless hotspot anqp-server** *server-name* **Example:** `Device(config)# wireless hotspot anqp-server my_server`	Configures a Hotspot 2.0 ANQP server.
Step 3	**network-type allowed** *network-type* **internet-access** { **allowed** | **forbidden** } **Example:** `Device(config-wireless-anqp-server)# network-type guest-private internet-access allowed`	Configures a 802.11u network type.
Step 4	**hessid** *HESSID-value* **Example:** `Device(config-wireless-anqp-server)# hessid 12.13.14`	(Optional) Configures a homogenous extended service set.
Step 5	**group** *venue-group venue-type* **Example:** `Device(config-wireless-anqp-server)# group business bank`	Selects a group type and venue type from the list of available options.

Configuring the Generic Advertisement Service Rate Limit

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:**	Configures an AP profile and enters AP profile configuration mode.

	Command or Action	Purpose
	`Device(config)# ap profile hs2-profile`	
Step 3	**gas-ap-rate-limit** *request-number interval* **Example:** `Device(config-ap-profile)# gas-ap-rate-limit 20 120`	Configures the number of Generic Advertisement Services (GAS) request action frames sent to the controller by an AP in a given interval.
Step 4	**exit** **Example:** `Device(config-ap-profile)# exit`	Returns to global configuration mode.
Step 5	**wireless hotspot gas-rate-limit** *gas-requests-to-process* **Example:** `Device(config)# wireless hotspot gas-rate-limit 100`	Configures the number of GAS request action frames to be processed by the controller.

Configuring Global Settings

Procedure

Step 1 Choose **Configuration > Wireless > Hotspot/OpenRoaming > Global Settings**.

Step 2 In the **Gas Rate Limit (Requests per sec)** field, enter the number of GAS request action frames to be processed by the controller.

Step 3 Go to the **Icons Configuration** area.

Step 4 Click **Add**.

The **Add Global Icon** window is displayed.

Step 5 From the **System Path** drop-down list, choose the path.

Step 6 In the **Icon Name** field, enter the icon name.

Step 7 In the **Icon Type** field, enter the icon type.

Step 8 In the **Language Code** field, enter the language code.

Step 9 In the **Icon Height** field, enter the icon height.

Step 10 In the **Icon Width** field, enter the icon width.

Step 11 Click **Apply to Device**.

Configuring Advice of Charge

Use the following procedure to configure the advice of charge information for using the SSID of the Network Access Identifier (NAI) realm.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless hotspot anqp-server** *server-name* **Example:** `Device(config)# wireless hotspot anqp-server my_server`	Configures a Hotspot 2.0 ANQP server.
Step 3	**advice-charge** *type* **Example:** `Device(config-wireless-anqp-server)# advice-charge data`	Configures advice of charge for data usage. Advice of charge provides information on the financial charges for using the SSID of the NAI realm.
Step 4	**plan** *language currency* **info** *plan-info-file* **Example:** `Device(config-anqp-advice-charge)# plan eng eur info bootflash:plan_eng.xml`	Configures advice of charge information, which includes language, currency, and plan information. **Note** You can configure up to 32 plans.
Step 5	**nai-realm** *nai-realm* **Example:** `Device(config-anqp-advice-charge)# nai-realm cisco`	Configures NAI realm for this advice of charge. **Note** You can configure up to 32 realms.

Configuring Terms and Conditions

Before you begin

Define a URL filter list, as shown in the following example:

```
urlfilter list <url-filter-name>
    action permit
    filter-type post-authentication
    url <allow-url>
```

For information on configuring an URL list, see the *Defining URL Filter List* section.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless hotspot anqp-server** *server-name* **Example:** `Device(config)# wireless hotspot anqp-server my_server`	Configures a Hotspot 2.0 ANQP server.
Step 3	**terms-conditions filename** *file-name* **Example:** `Device(config-wireless-anqp-server)# terms-conditions filename xyz-file`	Configures the terms and conditions filename for the clients.
Step 4	**terms-conditions timestamp** *date time* **Example:** `Device(config-wireless-anqp-server)# terms-conditions timestamp 2020-02-20 20:20:20`	Configures the terms and conditions timestamp.
Step 5	**terms-conditions urlfilter list** *url-filter-list* **Example:** `Device(config-wireless-anqp-server)# terms-conditions urlfilter list filter-yy`	Configures the terms and conditions URL filter list name.

Defining ACL and URL Filter in AP for FlexConnect

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	*sequence-number* **permit udp any eq bootpc any eq bootps** **Example:** `Device(config-ext-nacl)# 10 permit udp any eq bootpc any eq bootps`	Defines an extended UDP access list and sets the access conditions to match only the packets on a given port number of bootstrap protocol (BOOTP) clients from any source host to match only the packets on a given port number of the bootstrap protocol (BOOTP) server of a destination host.
Step 3	*sequence-number* **permit udp any eq bootps any eq bootpc** **Example:** `Device(config-ext-nacl)# 20 permit udp any eq bootps any eq bootpc`	Defines an extended UDP access list to forward packets and sets the access conditions to match only the packets on a given port number of bootstrap protocol (BOOTP) server from any source host to match only the packets of a given port number of the bootstrap protocol (BOOTP) clients of a destination host.

	Command or Action	Purpose
Step 4	*sequence-number* **permit udp any eq domain any eq domain** **Example:** `Device(config-ext-nacl)# 30 permit udp any eq domain any eq domain`	Defines an extended UDP access list to forward packets and sets the access conditions to match a destination host Domain Name Service (DNS) with only the packets from a given port number of the source DNS.
Step 5	*sequence-number* **permit ip any host** *dest-address* **Example:** `Device(config-ext-nacl)# 40 permit ip any host 10.10.10.8`	Defines an extended IP access list to forward packets from a source host to a single destination host.
Step 6	*sequence-number* **permit ip host** *dest-address* **any** **Example:** `Device(config-ext-nacl)# 50 permit ip host 10.10.10.8 any`	Defines an extended IP access list to forward packets from a single source host to a destination host.
Step 7	**exit** **Example:** `Device(config-ext-nacl)# exit`	Returns to global configuration mode.
Step 8	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test-flex-profile`	Configures a new FlexConnect policy and enters wireless flex profile configuration mode.
Step 9	**acl-policy** *acl-policy-name* **Example:** `Device(config-wireless-flex-profile)# acl-policy acl_name`	Configures an ACL policy.
Step 10	**urlfilter list** *url-filter-name* **Example:** `Device(config-wireless-flex-profile)# urlfilter list urllist_flex`	Applies the URL filter list to the FlexConnect profile.
Step 11	**vlan-name** *prod-vlanID* **Example:** `Device(config-wireless-flex-profile)# vlan-name test-vlan`	Configures a production VLAN. Ensure that **filter-type post-authentication** configuration is in place for the URL filter to work. For information on configuring URL filter list, see the *Defining URL Filter List* section of the chapter DNS-Based Access Control Lists.
Step 12	**vlan-id** *prod-vlanID* **Example:**	Creates a new production VLAN ID.

	Command or Action	Purpose
	`Device(config-wireless-flex-profile-vlan)# vlan-id 10`	
Step 13	**vlan-name** *OSU-vlanID* **Example:** `vlan-name test-vlan`	Configures an OSU VLAN.
Step 14	**vlan-id** *OSU-vlanID* **Example:** `vlan-id 20`	Creates an OSU VLAN ID.

Configuring an OSEN WLAN (Single SSID)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan hs2 1 hs2`	Configures a WLAN and enters WLAN configuration mode.
Step 3	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 4	**no security ft adaptive** **Example:** `Device(config-wlan)# no security ft adaptive`	Disables adaptive 11r.
Step 5	**security wpa wpa2** **Example:** `Device(config-wlan)# security wpa wpa2`	Enables WPA2 security.
Step 6	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Enables WPA2 ciphers for AES.
Step 7	**security wpa osen** **Example:**	Enables WPA OSEN security support.

	Command or Action	Purpose
	`Device(config-wlan)# security wpa osen`	
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**exit** **Example:** `Device(config-wlan)# exit`	Returns to global configuration mode.
Step 10	**wireless profile policy** *policy-profile-name ssid* **Example:** `Device(config)# wireless profile policy policy-hotspot`	Configures a policy profile.
Step 11	**hotspot anqp-server** *server-name* **Example:** `Device(config-wireless-policy)# hotspot anqp-server my-server`	Attaches the Hotspot 2.0 ANQP server to the policy profile.
Step 12	**vlan** *vlan* **encryption osen** **Example:** `Device(config-wireless-policy)# vlan 10 encryption osen`	Configures the VLAN ID with OSEN encryption for single SSID.

Verifying Hotspot 2.0 Configuration

Use the following **show** commands to verify the quality of service (QoS) and AP GAS rate limit.

To view whether a QoS map ID is user configured or the default one, use the following command:

```
Device# show ap profile <profile name> detailed

QoS Map                         : user-configured
```

To view the QoS map values used and their source, use the following command:

```
Device# show ap profile <profile name> qos-map

QoS Map                         : default
DSCP ranges to User Priorities
 User Priority   DSCP low   DSCP high   Upstream UP to DSCP
---------------------------------------------------------
             0          0           7                     0
             2         16          23                    10
             3         24          31                    18
             4         32          39                    26
             5         40          47                    34
             6         48          55                    46
             7         56          63                    48

DSCP to UP mapping exceptions
```

```
 DSCP   User Priority
---------------------
    0               0
    2               1
    4               1
    6               1
   10               2
   12               2
   14               2
   18               3
   20               3
   22               3
```

To view the AP rate limiter configuration, use the following command:

```
Device# show ap name AP0462.73e8.f2c0 config general | i GAS

GAS rate limit Admin status                     : Enabled
Number of GAS request per interval              : 30
GAS rate limit interval (msec)                  : 100
```

Verifying Client Details

To verify the wireless-specific configuration of active clients based on their MAC address, use the following command:

```
Device# show wireless client mac 001e.f64c.1eff detail
.
.
.
Hotspot version : Hotspot 2.0 Release 2
Hotspot PPS MO ID :
Hotspot Terms and Conditions URL :
http://host1.ciscohotspot.com/terms.php?addr=b8:27:eb:5a:dc:39&ap=123
.
.
.
Policy Type : OSEN (within RSN)
Resultant Policies:
    VLAN Name        : VLAN0010
    VLAN             : 10
```

CHAPTER 187

Client Roaming Across Policy Profile

- Information about Client Roaming Policy Profile, on page 2111
- Configuring Client Roaming Across Policy Profile, on page 2112
- Verifying Client Roaming Across Policy Profiles, on page 2113

Information about Client Roaming Policy Profile

In Cisco Catalyst 9800 Series Wireless controller, each WLAN must be associated to a policy profile using a policy tag. Since the policy profile represent the policy defined by the administrator, the general rule is that the controller will not allow seamless roaming between same WLAN associated with different policy profile. The client will be disconnected hence disrupting seamless roaming and client will be required to join again and the new policy can be evaluated and implemented.

When you enable roaming across policy profile, if the two policy profiles differ only in the settings as listed, then client seamless roaming is allowed to same wlan associated to different policy profiles.

A typical use case is when clients roaming across two APs that belong to different policy tag and have WLAN associated with different policy profiles with different VLAN setting for each policy profile. If roaming across policy profile is enabled, the controller allows seamless roaming to another policy profile even if the VLAN is different and the client retains the original IP address. The controller applies all other attributes except VLAN from the new policy profile to which client has joined.

Client roaming across policy profiles is not allowed if there are different policy profile configurations. However; the following are the exceptions:

- Accounting list
- CTS
- DHCP-TLV-caching
- Dot11 5 Ghz airtime-fairness
- Dot11 24 Ghz airtime-fairness
- ET-analytics enable
- http-TLV-caching
- Idle-threshold
- Idle-timeout

- MDnS-SD service policy
- IPv4 ACL
- IPv6 ACL
- QBSS load
- RADIUS profiling
- Session timeout
- SIP CAC disassociation client
- SIP CAC send-486busy
- VLAN

You must execute the configuration in the global configuration mode. When a client roam across policy profile is attempted, the roam is either a success or a failure. However; the total roam across policy profiles counter under client global statistics section increments. But when the roam across policy profile is denied then roam across policy profile deny delete reason counter is incremented.

Note This feature is not supported on fabric and on Cisco 9800 FlexConnect.

The following is an example in which case a client roams across policy profiles PP1 and PP2 will be denied.

```
wireless profile policy PP1
vlan 42
no shutdown
wireless profile policy PP2
aaa-override
vlan 43
no shutdown
```

Configuring Client Roaming Across Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enables configuration mode
Step 2	**wireless client vlan-persistent** **Example:** `Device(config) # wireless client vlan-persistent`	Enables client roaming across different policy profiles.
Step 3	**end** **Example:**	Ends the session.

	Command or Action	Purpose
	Device(config) # end	

Verifying Client Roaming Across Policy Profiles

The following shows the client roaming from policy profile PP1 configured with VLAN 42 to policy profile PP2 configured with VLAN 43.

The following is the sample output of the **show wireless client mac-address xxxx.xxxx.xxxx detail** command that shows the client is connected to policy profile PP1.

```
Device#show wireless client mac-address xxxx.xxxx.xxxx detail

Client MAC Address : xxxx.xxxx.xxxx
Client MAC Type : Universally Administered Address
Client IPv4 Address : 169.254.189.170
Client Username : cisco
AP MAC Address : xxxx.xxxx.xxxx
AP Name: vinks_ios
AP slot : 1
Client State : Associated
Policy Profile : PP1
Flex Profile : N/A
Wireless LAN Id: 3
WLAN Profile Name: prateekk_dot1x
Wireless LAN Network Name (SSID): prateekk_dot1x
BSSID : 0081.c4f6.6bfb
Connected For : 688 seconds
Protocol : 802.11ac
Channel : 161
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Re-Authentication Timeout : 1800 sec (Remaining time: 1112 sec)
Session Warning Time : Timer not running
Input Policy Name  : client-default
Input Policy State : Installed
Input Policy Source : QOS Internal Policy
Output Policy Name  : client-default
Output Policy State : Installed
Output Policy Source : QOS Internal Policy
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m8 ss1
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 07/13/2020 02:00:22 UTC
Client Join Time:
  Join Time Of Client : 07/13/2020 02:00:22 UTC
Client State Servers : None
```

```
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 688 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : EAP-FAST
VLAN Override after Webauth : No
VLAN : 42
Multicast VLAN : 0
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90400006
  IIF ID              : 0x90400006
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 3C2A09090000000E45E6D59E
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
   Server IP : 9.10.8.247
  Auth Method Status List
   Method : Dot1x
    SM State          : AUTHENTICATED
    SM Bend State     : IDLE
  Local Policies:
   Service Template : wlan_svc_PP1_local (priority 254)
    VLAN              : 42
    Absolute-Timer    : 1800
  Server Policies:
  Resultant Policies:
    VLAN Name         : VLAN0042
    VLAN              : 42
    Absolute-Timer    : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received from Client : 19442
  Number of Bytes Sent to Client : 3863
  Number of Packets Received from Client : 197
  Number of Packets Sent to Client : 36
  Number of Policy Errors : 0
```

```
  Radio Signal Strength Indicator : -39 dBm
  Signal to Noise Ratio : 55 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: None
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : Pending Classification
Device Type      : Apple-Device
Device Name      : APPLE, INC.
Protocol Map     : 0x000001  (OUI)
Max Client Protocol Capability: 802.11ac Wave 2
Cellular Capability : N/A
Apple Specific Requests(ASR) Capabilities/Statistics Summary
  Regular ASR support: : DISABLED
```

The following is the sample output of the **show wireless client mac-address xxxx.xxxx.xxxx detail** command after client has roamed to a policy profile PP2.

```
Client MAC Address : xxxx.xxxx.xxxx
Client MAC Type : Universally Administered Address
Client IPv4 Address : 9.9.42.236
Client Username : cisco
AP MAC Address : xxxx.xxxx.xxxx
AP Name: prateekk_cos_1
AP slot : 1
Client State : Associated
Policy Profile : PP2
Flex Profile : N/A
Wireless LAN Id: 3
WLAN Profile Name: prateekk_dot1x
Wireless LAN Network Name (SSID): prateekk_dot1x
BSSID : a0f8.4985.0029
Connected For : 11 seconds
Protocol : 802.11ac
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Re-Authentication Timeout : 1800 sec (Remaining time: 1789 sec)
Session Warning Time : Timer not running
Input Policy Name  : client-default
Input Policy State : Installed
Input Policy Source : QOS Internal Policy
Output Policy Name  : client-default
Output Policy State : Installed
Output Policy Source : QOS Internal Policy
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m9 ss3
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : L2
  Mobility Complete Timestamp : 07/13/2020 02:12:19 UTC
```

```
Client Join Time:
  Join Time Of Client : 07/13/2020 02:12:19 UTC
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 728 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : EAP-FAST
VLAN Override after Webauth : No
VLAN : 43
Multicast VLAN : 0
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90000005
  IIF ID              : 0x90000005
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 3C2A09090000000E45E6D59E
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
   Server IP : 9.10.8.247
  Auth Method Status List
   Method : Dot1x
    SM State          : AUTHENTICATED
    SM Bend State     : IDLE
  Local Policies:
   Service Template : vlan-42-template (priority 200)
    VLAN              : 42
   Service Template : wlan_svc_PP2_local (priority 254)
    Absolute-Timer    : 1800
  Server Policies:
  Resultant Policies:
    VLAN Name         : VLAN0042
    VLAN              : 42
    Absolute-Timer    : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received from Client : 23551
```

```
  Number of Bytes Sent to Client : 12588
  Number of Packets Received from Client : 239
  Number of Packets Sent to Client : 71
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -28 dBm
  Signal to Noise Ratio : 60 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: None
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
  prateekk_cos_1 (slot 1)
   antenna 0: 13 s ago ........ -25  dBm
   antenna 1: 13 s ago ........ -25  dBm
EoGRE : No/Simple client
Device Type      : Apple-Device
Device Name      : APPLE, INC.
Protocol Map     : 0x000001  (OUI)
Protocol         : DHCP
Type             : 0    0
Data             : 00

Max Client Protocol Capability: 802.11ac Wave 2
Cellular Capability : N/A
Apple Specific Requests(ASR) Capabilities/Statistics Summary
  Regular ASR support: : DISABLED
```

The following is the sample output of the **show wireless stats client detail** command that displays that client roam across policy profile is attempted and roam across policy is not denied.

```
Device #show wireless stats client detail | in Roam
Total Roam Across Policy Profiles : 1
Roam across policy profile deny : 0
```

CHAPTER 188

Assisted Roaming

- 802.11k Neighbor List and Assisted Roaming, on page 2119
- Restrictions for Assisted Roaming, on page 2120
- How to Configure Assisted Roaming, on page 2120
- Verifying Assisted Roaming, on page 2122
- Configuration Examples for Assisted Roaming, on page 2122

802.11k Neighbor List and Assisted Roaming

The 802.11k standard allows an AP to inform 802.11k-capable clients of neighboring BSSIDs (APs in the same SSID). This can help the client to optimize its scanning and roaming behavior. Additionally, the Assisted Roaming Prediction Optimization feature can be used with non-802.11k clients, to discourage them from roaming to suboptimal APs.

Note We recommend not configuring two SSIDs with the same name in the controller, which may cause roaming issues.

Prediction Based Roaming - Assisted Roaming for Non-802.11k Clients

You can optimize roaming for non-802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request. When prediction based roaming enables a WLAN, after each successful client association/re-association, the same neighbor list optimization applies on the non-802.11k client to generate and store the neighbor list in the mobile station software data structure. Clients at different locations have different lists because the client probes are seen with different RSSI values by the different neighbors as the clients usually probe before any association or re-association. This list is created with the most updated probe data and predicts the next AP that the client is likely to roam to.

The wireless infrastructure discourages clients from roaming to those less desirable neighbors by denying association if the association request to an AP does not match the entries on the stored prediction neighbor list.

- Denial count: Maximum number of times a client is refused association.
- Prediction threshold: Minimum number of entries required in the prediction list for the assisted roaming feature to activate.

For more information, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/Chapter-11.html#pgfId-1140097.

Restrictions for Assisted Roaming

- This feature is supported only on 802.11n capable indoor access points. For a single band configuration, a maximum of 6 neighbors are visible in a neighbor list. For dual band configuration, a maximum of 12 neighbors are visible.
- You can configure assisted roaming only using the device CLI.

How to Configure Assisted Roaming

Configuring Assisted Roaming (GUI)

Assisted roaming allows clients to request neighbor reports containing information about known neighbor access points that are candidates for a service set transition.

Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLAN** and click **Add** to add a WLAN or select an existing WLAN.

Step 2 On the **Advanced** tab, go to the **Assisted Roaming (11K)** and select the **Prediction Optimization** checkbox to optimize roaming for non 802.11k clients by generating a prediction neighbor list for each client without sending an 802.11k neighbor list request.

Step 3 Select the **Neighbor List** checkbox to optimize roaming for 802.11K clients by generating a neighbor list for each client without sending an 802.11k neighbor list request. By default, the neighbor list contains only neighbors in the same band with which the client is associated. However, if you select the Dual Band Neighbor List checkbox, it allows 802.11k to return neighbors in both bands.

Step 4 Click **Apply to Device.** .

Configuring Assisted Roaming (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless assisted-roaming floor-bias** *dBm* **Example:** `Device(config)# wireless assisted-roaming floor-bias 20`	Configures neighbor floor label bias. The valid range is from 5 to 25 dBm, and the default value is 15 dBm.
Step 3	**wlan** *wlan-id* **Example:** `Device(config)# wlan wlan1`	Enters the WLAN configuration submode. The *wlan-name* is the profile name of the configured WLAN.
Step 4	**assisted-roaming neighbor-list** **Example:** `Device(wlan)# assisted-roaming neighbor-list`	Configures an 802.11k neighbor list for a WLAN. By default, assisted roaming is enabled on the neighbor list when you create a WLAN. The **no** form of the command disables assisted roaming neighbor list.
Step 5	**assisted-roaming dual-list** **Example:** `Device(wlan)# assisted-roaming dual-list`	Configures a dual-band 802.11k dual list for a WLAN. By default, assisted roaming is enabled on the dual list when you create a WLAN. The **no** form of the command disables assisted roaming dual list.
Step 6	**assisted-roaming prediction** **Example:** `Device(wlan)# assisted-roaming prediction`	Configures assisted roaming prediction list feature for a WLAN. By default, the assisted roaming prediction list is disabled. **Note** A warning message is displayed and load balancing is disabled for the WLAN if load balancing is already enabled for the WLAN.
Step 7	**wireless assisted-roaming prediction-minimum** *count* **Example:** `Device# wireless assisted-roaming prediction-minimum`	Configures the minimum number of predicted APs required for the prediction list feature to be activated. The default value is 3. **Note** If the number of the AP in the prediction assigned to the client is less than the number that you specify, the assisted roaming feature will not apply on this roam.

	Command or Action	Purpose
Step 8	**wireless assisted-roaming denial-maximum** *count* **Example:** `Device# wireless assisted-roaming denial-maximum 8`	Configures the maximum number of times a client can be denied association if the association request is sent to an AP does not match any AP on the prediction. The valid range is from 1 to 10, and the default value is 5.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Assisted Roaming

The following command can be used to verify assisted roaming configured on a WLAN:

Command	Description
show wlan id *wlan-id*	Displays the WLAN parameters on the WLAN.

Configuration Examples for Assisted Roaming

This example shows how to configure the neighbor floor label bias:

```
Device# configure terminal
Device(config)# wireless assisted-roaming floor-bias 10
Device(config)# end
Device# show wlan id 23
```

This example shows how to disable neighbor list on a specific WLAN:

```
Device# configure terminal
Device(config)# wlan test1
Device(config (wlan)# no assisted-roaming neighbor-list
Device(config)(wlan)# end
Device# show wlan id 23
```

This example shows how to configure the prediction list on a specific WLAN:

```
Device# configure terminal
Device(config)# wlan test1
Device(config)(wlan)# assisted-roaming prediction
Device(config)(wlan)# end
Device# show wlan id 23
```

This example shows how to configure the prediction list based on assisted roaming prediction threshold and maximum denial count on a specific WLAN:

```
Device# configure terminal
Device(config)# wireless assisted-roaming prediction-minimum 4
```

```
Device(config)# wireless assisted-roaming denial-maximum 4
Device(config)(wlan)# end
Device# show wlan id 23
```

CHAPTER 189

802.11r BSS Fast Transition

- Feature History for 802.11r Fast Transition, on page 2125
- Information About 802.11r Fast Transition, on page 2126
- Information About 802.11r Fast Transition for SAE (FT-SAE) Authenticated Clients, on page 2127
- Restrictions for 802.11r Fast Transition, on page 2128
- Monitoring 802.11r Fast Transition (CLI), on page 2129
- Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 2130
- Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 2131
- Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI), on page 2133
- Configuring 802.11r Fast Transition on a SAE Security-Enabled WLAN (GUI), on page 2134
- Configuring 802.11r Fast Transition on an SAE Security-Enabled WLAN (CLI), on page 2134
- Disabling 802.11r Fast Transition (GUI), on page 2136
- Disabling 802.11r Fast Transition (CLI), on page 2136
- Verifying 802.11r Fast Transition SAE, on page 2136

Feature History for 802.11r Fast Transition

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 144: Feature History for 802.11r Fast Transition

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	802.11r Fast Transition for SAE (FT-SAE) Authenticated Clients	From Cisco-IOS XE 17.9.1 release onwards, the Fast Transition supports SAE-based Fast Roaming support along with PMK caching. This feature is an addition to the existing PMK caching-based fast roam support.

Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition. The initial handshake allows a client and the access points to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and the access points after the client responds to the reassociation request or responds to the exchange with new target AP.

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

Client Roaming

For a client to move from its current AP to a target AP using the FT protocols, message exchanges are performed using one of the following methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-Distribution System (DS)—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the device.

Figure 57: Message Exchanges when Over–the–Air Client Roaming is Configured

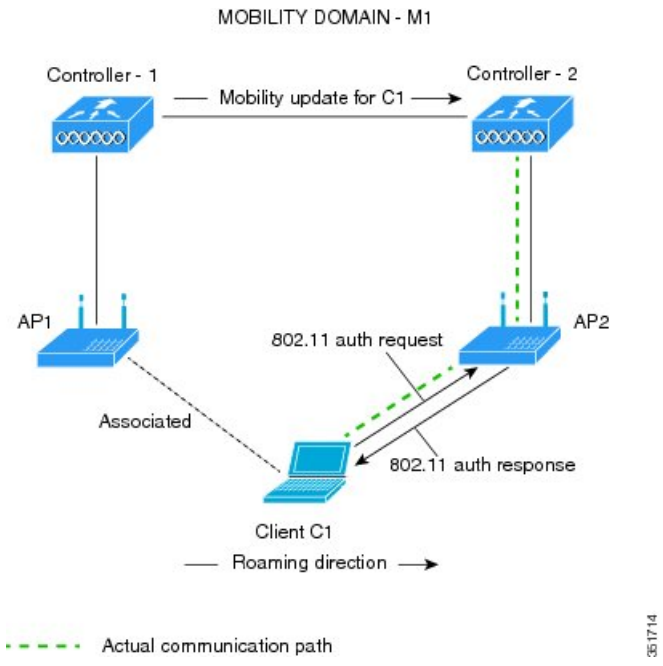
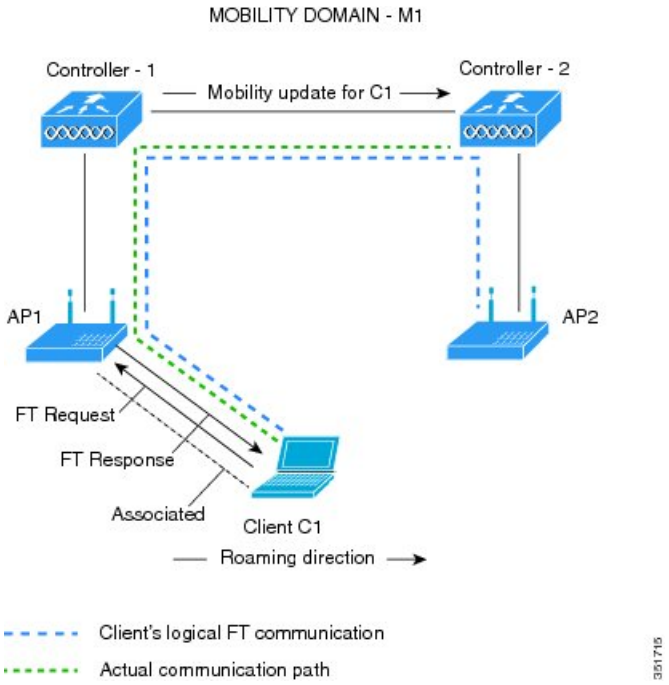


Figure 58: Message Exchanges when Over–the–DS Client Roaming is Configured



Note The 802.11r Fast Transition for SAE (FT-SAE) is not restricted to inter controller roaming.

Information About 802.11r Fast Transition for SAE (FT-SAE) Authenticated Clients

From Cisco-IOS XE 17.9.1 release onwards, the Fast Transition feature supports Simultaneous Authentication of Equals-based (SAE-based) fast roaming support along with Pairwise Master Key (PMK) caching.

This feature is an addition to the existing PMK caching-based fast roaming support.

Fast Transition Protocol

During a Base Station Subsystem (BSS) transition, the Fast BSS transition feature reduces the connectivity time loss between an Station (STA) and Direct Switching. The Fast Transition protocols are part of the reassociation service, and apply to the STA transitions between the APs in the same mobility domain and Exteneded Service Set (ESS). The Fast Transition protocols need information to be exchanged during the initial association (or a later reassociation) between an STA and an AP. The initial exchange is referred to as the *FT initial mobility domain association*. Similarly, subsequent reassociations to the APs in the same mobility domain use the Fast Transition protocols.

Note STA is known as Fast Transition Originator.

The following are the FT protocols:

- **Fast Transition Protocol**: This protocol is executed when a Fast Transition Originator makes a transition to a target AP and does not require a resource request before its transition.
- **Fast Transition Resource Request Protocol**: This protocol is executed when a Fast Transition Originator requires a resource request prior to its transition.
- **Over-the-Air**: The Fast Transition Originator communicates with the target AP using IEEE 802.11 authentication with Fast Transition authentication algorithm.
- **Over-the-DS**: The Fast Transition Originator communicates with the target AP using the current AP. The communication between the Fast Transition Originator and target AP is carried in Fast Transition action frames between the Fast Transition Originator and the current AP.

The Fast Transition feature supports a new AKM for FT-SAE, specifically the **00-0F-AC:9**.

Fast Transition Initial Mobility Domain Association

An STA includes Mobility Domain Element (MDE) and Robust Security Network Element (RSNE) in the (re)association request frame. The AP responds by including FTE, MDE, and RSNE in the (re)association response frame.

That is, an STA initiates the Fast Transition initial mobility domain association procedures by performing an IEEE 802.11 authentication using the SAE algorithm.

After successful SAE authentication, the STA and AP perform a Fast Transition four-way handshake.

Note

- If the MDE that is received by an AP or a controller does not match the contents advertised in the beacon and probe response frames, the AP or controller rejects the (re)association request frame with the STATUS_INVALID_MDE code.
- If an MDE is available in the (re)association request frame and the contents of RSNE do not indicate a negotiated SAE AKM of Fast BSS Transition (00-0F-AC:9 suite type), the AP rejects with STATUS_INVALID_AKMP code.

After an SAE authentication, the controller receives the PMK, resulting in the successful completion of SAE.

Restrictions for 802.11r Fast Transition

- EAP LEAP method is not supported.
- Traffic Specification (TSPEC) is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.

- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The Cisco WLC handles 802.11r Fast Transition authentication requests during roaming for both Over-the-Air and Over-the-DS methods.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r-capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r-enabled WLANs.

  Another workaround is to have two SSIDs with the same name, but with different security settings (FT and non-FT).
- Fast Transition resource–request protocol is not supported because clients do not support this protocol. Also, the resource–request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.
- Non-802.11r–capable devices will not be able to associate with FT-enabled WLAN.
- We do not recommend 802.11r FT + PMF.
- We recommend 802.11r FT Over-the-Air roaming for FlexConnect deployments.
- FT-SAE Over-the-DS roam is not supported in FlexConnect local authentication mode.
- 802.11r ft-over-ds is enabled by default, when a WLAN is created in the controller . In Cisco Wave 2 APs, local switching local authentication with 802.11r is not supported. To make the local switching local authentication work with Cisco Wave 2 APs, explicitly disable 802.11r in WLAN. A sample configuration is given below:

```
wlan local-dot1x 24 local-dot1x
no security ft over-the-ds
no security ft adaptive
security dot1x authentication-list spwifi_dot1x
no shutdown
```

Monitoring 802.11r Fast Transition (CLI)

The following command can be used to monitor 802.11r Fast Transition:

Command	Description
show wlan name *wlan-name*	Displays a summary of the configured parameters on the WLAN.

Command	Description
show wireless client mac-address *mac-address*	Displays the summary of the 802.11r authentication key management configuration on a client. . . . . . . Client Capabilities CF Pollable : Not implemented CF Poll Request : Not implemented Short Preamble : Not implemented PBCC : Not implemented Channel Agility : Not implemented Listen Interval : 15 Fast BSS Transition : Implemented Fast BSS Transition Details : Client Statistics: Number of Bytes Received : 9019 Number of Bytes Sent : 3765 Number of Packets Received : 130 Number of Packets Sent : 36 Number of EAP Id Request Msg Timeouts : 0 Number of EAP Request Msg Timeouts : 0 Number of EAP Key Msg Timeouts : 0 Number of Data Retries : 1 Number of RTS Retries : 0 Number of Duplicate Received Packets : 1 Number of Decrypt Failed Packets : 0 Number of Mic Failured Packets : 0 Number of Mic Missing Packets : 0 Number of Policy Errors : 0 Radio Signal Strength Indicator : -48 dBm Signal to Noise Ratio : 40 dB . . . . . .

Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**client vlan** *vlan-name* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to this WLAN.
Step 4	**local-auth** *local-auth-profile-eap* **Example:** `Device(config-wlan)# local-auth`	Enables the local auth EAP profile.
Step 5	**security dot1x authentication-list default** **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 6	**security ft** **Example:** `Device(config-wlan)# security ft`	Enables 802.11r Fast Transition on the WLAN.
Step 7	**security wpa akm ft dot1x** **Example:** `Device(config-wlan)# security wpa akm ft dot1x`	Enables 802.1x security on the WLAN.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Configuring 802.11r Fast Transition in an Open WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**client vlan** *vlan-id* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to the WLAN.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**no wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**security ft** **Example:** `Device(config-wlan)# security ft`	Specifies the 802.11r Fast Transition parameters.
Step 9	**no shutdown** **Example:** `Device(config-wlan)# shutdown`	Shuts down the WLAN.
Step 10	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-name* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to this WLAN.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa akm ft psk** **Example:** `Device(config-wlan)# security wpa akm ft psk`	Configures Fast Transition PSK support.
Step 6	**security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}} **Example:** `Device(config-wlan)# security wpa akm psk set-key ascii 0 test`	Configures PSK AKM shared key.
Step 7	**security ft** **Example:** `Device(config-wlan)# security ft`	Configures 802.11r Fast Transition.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Configuring 802.11r Fast Transition on a SAE Security-Enabled WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab.

Step 5 Click the **WPA3** radio button as security mode.

Step 6 Check the required **WPA Parameters** check boxes and the **AES(CCMP128)** check box.

Step 7 From the **Status** drop-down list, choose **Enabled**.

Step 8 Check the **FT+SAE** check box.

Step 9 Enter the **Pre-Shared Key**.

Step 10 From the **PSK Format** drop-down list, choose PSK Format and from the **PSK Type** drop-down list, choose PSK Type.

Step 11 Click **Apply to Device**.

Configuring 802.11r Fast Transition on an SAE Security-Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enables configuration mode.

	Command or Action	Purpose
Step 3	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan wlan-ft-sae 10 wlan-ft-sae`	Configures the WLAN and SSID.
Step 4	**security ft** **Example:** `Device(config-wlan)# security ft`	Enables 802.11r Fast Transition on the WLAN.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**security wpa psk set-key ascii** *asciii/hex key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 123456789`	Configures the preshared key on a WLAN. **Note** WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
Step 7	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 8	**security wpa akm ft sae** **Example:** `Device(config-wlan)# security wpa akm ft sae`	Configures 802.11r Fast Transition on an SAE security–enabled WLAN.
Step 9	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 10	**security pmf mandatory** **Example:** `Device(config-wlan)# security pmf mandatory`	Requires clients to negotiate 802.11w PMF protection on a WLAN.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Disabling 802.11r Fast Transition (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the WLAN name.

Step 3 In the **Edit WLAN** window, click the **Security** > **Layer2** tab.

Step 4 From the **Fast Transition** drop-down list, choose **Disabled**. Note that you cannot enable or disable Fast Transition, if you have configured an SSID with Open Authentication.

Step 5 Click **Update & Apply to Device**.

Disabling 802.11r Fast Transition (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables 802.11r Fast Transition on the WLAN.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying 802.11r Fast Transition SAE

To view the Fast Transition SAE details, use the following command:

```
Device# show wireless client summary
Number of Clients: 1
```

```
MAC Address AP Name Type ID State Protocol Method Role
------------------------------------------------------------------------------------------------
2c33.7a5b.8fc5 APF4BD.9EBD.A66C WLAN 10 Run 11n(2.4) FT-SAE Local

Number of Excluded Clients: 0
```

To view the client summary details from an AP, use the following command:

```
AP# show client summary

Radio Driver client Summary:
============================
apr0v1
-------
apr0v4
-------
ADDR AID CHAN TXRATE RXRATE RSSI MINRSSI MAXRSSI IDLE TXSEQ RXSEQ CAPS XCAPS ACAPS ERP STATE
 MAXRATE(DOT11) HTCAPS VHTCAPS ASSOCTIME IEs MODE RXNSS TXNSS PSMODE
a0:fb:c5:ab:c3:41 1 11 114M 97M -47 -60 -40 0 0 65535 EPSs BORI NULL 0 f 286800 AP 1g
00:19:53 RSN WME IEEE80211_MODE_11AXG_HE20 2 2 1
LM BRP BRA
RSSI is combined over chains in dBm
Minimum Tx Power : 0
Maximum Tx Power : 0
HT Capability : Yes
VHT Capability : No
MU capable : No
SNR : 48
Operating band : 2.4GHz
Current Operating class : 0
Supported Rates : 2 4 11 22 12 18 24 36 48 72 96 108
Channels supported : 2412 2417 2422 2427 2432 2437 2442 2447 2452 2457 2462 2467 2472
Max STA phymode : IEEE80211_MODE_11AXG_HE20
apr1v1
-------
apr1v4
-------

WCP client Summary:
===================
mac radio vap aid state encr Maxrate Assoc Cap is_wgb_wired wgb_mac_addr
A0:FB:C5:AB:C3:41 0 4 1 FWD AES_CCM128 MCS92SS HE HE false 00:00:00:00:00:00



Assoc time:
============
mac assoc_time
A0:FB:C5:AB:C3:41 00d:00h:19m:55s


Datapath IPv4 client Summary:
=============================
id vap port node tunnel mac seen_ip hashed_ip sniff_ago confirm_ago
A0:FB:C5:AB:C3:41 4 apr0v4 6.4.26.28 - A0:FB:C5:AB:C3:41 192.100.2.153 10.0.21.68 0.110000
 0.100000

Datapath IPv6 client Summary:
=============================
client mac seen_ip6 age scope port
1 A0:FB:C5:AB:C3:41 fe80::c2f:f0c4:9fa5:2608 1 link-local apr0v4
```

To view FlexConnect-related details from an AP, use the following command:

```
AP# show flexconnect dot11R

Total number of DOT11R cache entries: 1

HW Address Life Time(s) BSSID R0KhId R1KhId vlanOverride aclOverride ipv6AclOverride
qosOverride iPSK
A0:FB:C5:AB:C3:41 558 2C:57:41:59:F5:C4 239.13.224.36 45:49:7B:38:11:6A N/A 0 \<>
```

To view the authentication key management details, use the following command:

```
Device# show wireless client mac-address 28c2.1f54.e6d6 detail
Authentication Algorithm : Open System
Authentication Key Management : FT-SAE
FlexConnect Authentication : Central
```

To verify whether AKM Fast Transition-SAE is enabled or not, use the following command:

```
Device# show wlan name [wlan-profile-name]

Auth Key Management
FT SAE : [Enabled | Disabled]
```

To verify the PMK cache details, use the following command:

```
Device# show wireless pmk-cache
……..
Type Dot11R
……..
```

To view the WPA3 SAE details, use the following command:

```
Device# show wireless stats client detail

Total FT/LocalAuth requests                      : 20
Total 11r ft authentication requests received    : 9
Total 11r ft authentication response success     : 9
Total 11r ft authentication response failure     : 0
Total 11r ft action requests received            : 17
Total 11r ft action response success             : 8
Total 11r ft action response failure             : 9
Total 11r PMKR0-Name mismatch                    : 0
Total 11r PMKR1-Name mismatch                    : 5
Total 11r MDID mismatch                          : 9
Total roam attempts                              : 15
  Total 11r roam attempts                        : 15
……
……
Total WPA3 SAE attempts                          : 0
Total WPA3 SAE successful authentications        : 0
Total WPA3 SAE authentication failures           : 0
  Total incomplete protocol failures             : 0
Total WPA3 SAE commit messages received          : 0
Total WPA3 SAE commit messages rejected                                    : 0
  Total unsupported group rejections                                       : 0
  Total PWE method mismatch for SAE Hash to Element commit received        : 0
Total PWE method mismatch for SAE Hunting And Pecking commit received : 0
Total WPA3 SAE commit messages sent              : 0
Total WPA3 SAE confirm messages received         : 0
Total WPA3 SAE confirm messages rejected         : 0
  Total WPA3 SAE message confirm field mismatch  : 0
  Total WPA3 SAE confirm message invalid length  : 0
Total WPA3 SAE confirm messages sent             : 0
Total WPA3 SAE Open Sessions                     : 0
Total SAE Message drops due to throttling        : 0
Total WPA3 SAE Hash to Element commit received   : 0
Total WPA3 SAE Hunting and Pecking commit received : 0
```

```
……
……
Total Flexconnect local-auth roam attempts       : 8
  Total 11r flex roam attempts                   : 0
…..
….
Total client delete reasons
  SAE authentication failure                                    : 0
  DOT11 SAE invalid message                                     : 0
```

CHAPTER 190

802.11v

- Information About 802.11v, on page 2141
- Prerequisites for Configuring 802.11v, on page 2142
- Restrictions for 802.11v, on page 2142
- Enabling 802.11v BSS Transition Management, on page 2142
- Configuring 802.11v BSS Transition Management (GUI), on page 2143
- Configuring 802.11v BSS Transition Management (CLI), on page 2143

Information About 802.11v

The controller supports 802.11v amendment for wireless networks, which describes numerous enhancements to wireless network management.

One such enhancement is Network assisted Power Savings which helps clients to improve the battery life by enabling them to sleep longer. As an example, mobile devices typically use a certain amount of idle period to ensure that they remain connected to access points and therefore consume more power when performing the following tasks while in a wireless network.

Another enhancement is Network assisted Roaming which enables the WLAN to send requests to associated clients, advising the clients as to better APs to associate to. This is useful for both load balancing and in directing poorly connected clients.

Enabling 802.11v Network Assisted Power Savings

Wireless devices consume battery to maintain their connection to the clients, in several ways:

- By waking up at regular intervals to listen to the access point beacons containing a DTIM, which indicates buffered broadcast or multicast traffic that the access point delivers to the clients.
- By sending null frames to the access points, in the form of keepalive messages– to maintain connection with access points.
- Devices also periodically listen to beacons (even in the absence of DTIM fields) to synchronize their clock to that of the corresponding access point.

All these processes consume battery and this consumption particularly impacts devices (such as Apple), because these devices use a conservative session timeout estimation, and therefore, wake up often to send keepalive messages. The 802.11 standard, without 802.11v, does not include any mechanism for the controller or the access points to communicate to wireless clients about the session timeout for the local client.

To save the power of clients due to the mentioned tasks in wireless network, the following features in the 802.11v standard are used:

- Directed Multicast Service
- Base Station Subsystem (BSS) Max Idle Period

Directed Multicast Service

Using Directed Multicast Service (DMS), the client requests the access point to transmit the required multicast packet as unicast frames. This allows the client to receive the multicast packets it has ignored while in sleep mode and also ensures Layer 2 reliability. Furthermore, the unicast frame is transmitted to the client at a potentially higher wireless link rate which enables the client to receive the packet quickly by enabling the radio for a shorter duration, thus also saving battery power. Since the wireless client also does not have to wake up at each DTIM interval in order to receive multicast traffic, longer sleeping intervals are allowed.

BSS Max Idle Period

The BSS Max Idle period is the timeframe during which an access point (AP) does not disassociate a client due to nonreceipt of frames from the connected client. This helps ensure that the client device does not send keepalive messages frequently. The idle period timer value is transmitted using the association and reassociation response frame from the access point to the client. The idle time value indicates the maximum time that a client can remain idle without transmitting any frame to an access point. As a result, the clients remain in sleep mode for a longer duration without transmitting the keepalive messages often. This in turn contributes to saving battery power.

Prerequisites for Configuring 802.11v

- Applies for Apple clients like Apple iPad, iPhone, and so on, that run on Apple iOS version 7 or later.
- Supports local mode; also supports FlexConnect access points in central authentication modes only.

Restrictions for 802.11v

Client needs to support 802.11v BSS Transition.

Enabling 802.11v BSS Transition Management

802.11v BSS Transition is applied in the following three scenarios:

- Solicited request—Client can send an 802.11v Basic Service Set (BSS) Transition Management Query before roaming for a better option of AP to reassociate with.
- Unsolicited Load Balancing request—If an AP is heavily loaded, it sends out an 802.11v BSS Transition Management Request to an associated client.
- Unsolicited Optimized Roaming request—If a client's RSSI and rate do not meet the requirements, the corresponding AP sends out an 802.11v BSS Transition Management Request to this client.

Note 802.11v BSS Transition Management Request is a suggestion (or advice) given to a client, which the client can choose to follow or ignore. To force the task of disassociating a client, turn on the disassociation-imminent function. This disassociates the client after a period if the client is not reassociated to another AP.

Configuring 802.11v BSS Transition Management (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add** to create WLANs.

The **Add WLAN** page is displayed.

Step 3 In the **Advanced** tab and **11v BSS Transition Support** section, select the **BSS Transition** check box to enable BSS transition per WLAN.

Step 4 Enable the **Dual Neighbor List** check box to include the neighbors of other radio slots of the same AP in the BSS transition response.

Note This is applicable only for 2.4 GHz and 5 GHz radio slots.

Step 5 Enable the **BSS Max Idle Service** check box to help clients and APs efficiently decide how long to remain associated when no traffic is being transmitted. The device uses this information to preserve device battery life.

Step 6 Enable the **BSS Max Idle Protected** check box to enable the AP to accept only authenticated frames (encrypted with Robust Security Network (RSN) information) from the client to reset the BSS Max Idle period counter. Without protected mode, any data or management frame (encrypted or unencrypted) sent by the client will reset the idle timer for the client.

Step 7 Enable the **Directed Multicast Service** check box to request the AP to send a multicast stream as unicast, to any DMS capable client on this WLAN.

Step 8 Click **Save & Apply to Device**.

Configuring 802.11v BSS Transition Management (CLI)

802.11v BSS Transtion is applied in the following three scenarios:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *profile-name* **Example:** `Device(config)# wlan test-wlan`	Configures WLAN profile and enters the WLAN profile configuration mode.
Step 3	**shut** **Example:** `Device(config-wlan)# shut`	Shutdown the WLAN profile.
Step 4	**bss-transition** **Example:** `Device(config-wlan)# bss-transition`	Configure BSS transition per WLAN.
Step 5	**bss-transition disassociation-imminent** **Example:** `Device(config-wlan)# bss-transition disassociation-imminent`	Configure BSS transition disassociation Imminent per WLAN.
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN profile.
Step 7	**end** **Example:** `Device(config-wlan)# end`	Return to privilege EXEC mode. Alternatively, you can press **CTRL + Z** to exit global configuration mode.

PART XVIII

Cisco DNA Service for Bonjour

- Cisco DNA Service for Bonjour Solution Overview, on page 2147
- Configuring Local and Wide Area Bonjour Domains, on page 2159
- Configuring Local Area Bonjour for Wireless Local Mode, on page 2201
- Configuring Local Area Bonjour for Wireless FlexConnect Mode, on page 2221
- Configuration Example for Local Mode - Wireless and Wired, on page 2245
- Configuration Example for FlexConnect Mode - Wireless and Wired, on page 2263

CHAPTER 191

Cisco DNA Service for Bonjour Solution Overview

- About the Cisco DNA Service for Bonjour Solution, on page 2147
- Solution Components, on page 2148
- Supported Platforms, on page 2149
- Supported Network Design, on page 2150

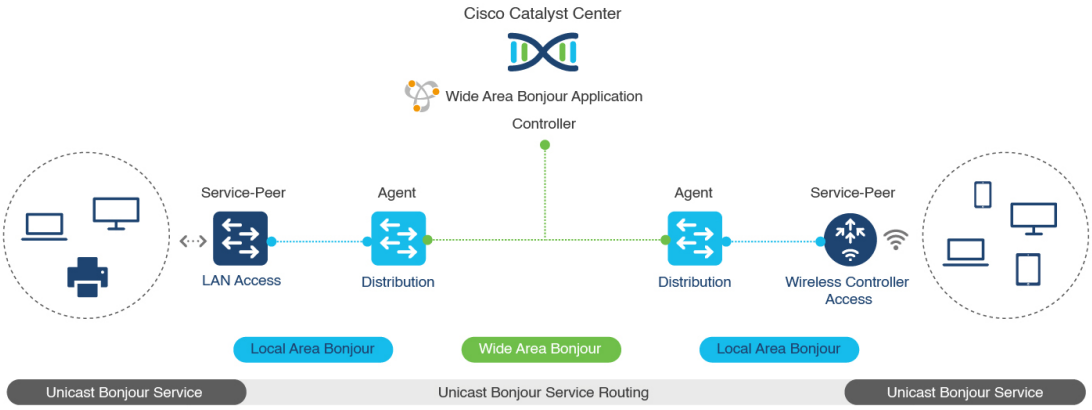
About the Cisco DNA Service for Bonjour Solution

The Apple Bonjour protocol is a zero-configuration solution that simplifies rich services and enables intuitive experience between connected devices, services, and applications. Using Bonjour, you can discover and use IT-managed, peer-to-peer, audio and video, or Internet of Things (IoT) services with minimal intervention and technical knowledge. Bonjour is originally designed for single Layer 2 small to mid-size networks, such as home or branch networks. The Cisco DNA Service for Bonjour solution eliminates the single Layer 2 domain constraint and expands the matrix to enterprise-grade traditional wired and wireless networks, including overlay networks such as Cisco Software-Defined Access (SD-Access) and industry-standard BGP EVPN with VXLAN. The Cisco Catalyst 9000 Series LAN switches, Cisco Nexus 9300 Series Switches, and Cisco Catalyst 9800 Series Wireless Controller follow the industry standard, RFC 6762-based multicast DNS (mDNS) specification to support interoperability with various compatible wired and wireless consumer products in enterprise networks.

The Cisco Wide Area Bonjour application on Catalyst Center enables mDNS service routing to advertise and discover services across enterprise-grade wired and wireless networks. The new-distributed architecture is designed to eliminate mDNS flood boundaries and transition to unicast-based service routing, providing policy enforcement points and enabling the management of Bonjour services.

The following figure illustrates how the Cisco Wide Area Bonjour application operates across two integrated service-routing domains.

Figure 59: Cisco Wide Area Bonjour Solution Architecture



- **Local Area Service Discovery Gateway Domain - Unicast Mode**: The new enhanced Layer 2 unicast policy-based deployment model. The new mDNS service discovery and distribution using the Layer 2 unicast address enables flood-free LAN and wireless networks. Cisco Catalyst 9000 Series Switches and Cisco Catalyst 9800 Series Wireless Controller in Layer 2 mode introduce a new service-peer role, replacing the classic flood-n-learn, for new unicast-based service routing support in the network. The service-peer switch and wireless controller also replace mDNS flood-n-learn with unicast-based communication with any RFC 6762 mDNS-compatible wired and wireless endpoints.
- **Wide-Area Service Discovery Gateway Domain**: The Wide Area Bonjour domain is a controller-based solution. The Bonjour gateway role and responsibilities of Cisco Catalyst and Cisco Nexus 9300 Series Switches are extended from a single SDG switch to an SDG agent, enabling Wide Area Bonjour service routing beyond a single IP gateway. The network-wide distributed SDG agent devices establish a lightweight, stateful, and reliable communication channel with a centralized Catalyst Center controller running the Cisco Wide Area Bonjour application. The SDG agents route locally discovered services based on the export policy.

Note The classic Layer 2 multicast flood-n-learn continues to be supported on wired and wireless networks with certain restrictions to support enhanced security and location-based policy enforcement. The Cisco Catalyst and Cisco Nexus 9300 Series Switches at Layer 3 boundary function as an SDG to discover and distribute services between local wired or wireless VLANs based on applied policies.

Solution Components

The Cisco DNA Service for Bonjour solution is an end-to-end solution that includes the following key components and system roles to enable unicast-based service routing across the local area and Wide Area Bonjour domain:

- **Cisco Service Peer**: Cisco Catalyst Switches and Cisco Wireless Controllers in Layer 2 access function in service peer mode to support unicast-based communication with local attached endpoints and export service information to the upstream Cisco Catalyst SDG agent in the distribution layer.

Note Cisco Nexus 9300 Series Switches don't support unicast-based service routing with downstream Layer 2 access network devices.

- **Cisco SDG Agent**: Cisco Catalyst and Cisco Nexus 9300 Series Switches function as an SDG agent and communicate with the Bonjour service endpoints in Layer 3 access mode. At the distribution layer, the SDG agent aggregates information from the downstream Cisco service peer switch and wireless controller, or local Layer 2 networks, and exports information to the central Catalyst Center controller.

Note Cisco Nexus 9300 Series Switches don't support multilayer LAN-unicast deployment mode.

- **Catalyst Center controller**: The Catalyst Center controller builds the Wide Area Bonjour domain with network-wide and distributed trusted SDG agents using a secure communication channel for centralized services management and controlled service routing.
- **Endpoints**: A Bonjour endpoint is any device that advertises or queries Bonjour services conforming to RFC 6762. The Bonjour endpoints can be in either LANs or WLANs. The Cisco Wide Area Bonjour application is designed to integrate with RFC 6762-compliant Bonjour services, including AirPlay, Google Chrome cast, AirPrint, and so on.

Supported Platforms

The following table lists the supported controllers, along with the supported hardware and software versions.

Table 145: Supported Controllers with Supported Hardware and Software Versions

Supported Controller	Hardware	Software Version
Catalyst Center appliance	DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL	Catalyst Center, Release 2.3.6
Cisco Wide Area Bonjour application	—	2.4.660.75403

The following table lists the supported SDG agents along with their licenses and software requirements.

Table 146: Supported SDG Agents with Supported License and Software Requirements

Supported Platform	Supported Role	Local Area SDG	Wide Area SDG	Minimum Software
Cisco Catalyst 9200 Series Switches	SDG agent Service peer	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1

Supported Platform	Supported Role	Local Area SDG	Wide Area SDG	Minimum Software
Cisco Catalyst 9200L Series Switches	SDG agent Service peer	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1
Cisco Catalyst 9300 and 9300-X Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1
Cisco Catalyst 9400 and 9400-X Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1
Cisco Catalyst 9500 and 9500-X Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1
Cisco Catalyst 9500 High Performance Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1
Cisco Catalyst 9600 and 9600-X Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1
Cisco Catalyst 9800 Wireless Controller	Service peer	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1
Cisco Catalyst 9800-L Wireless Controller	Service peer	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Release 17.11.1
Cisco Nexus 9300 Series Switches	SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco NX-OS Release 10.2(3)F

Supported Network Design

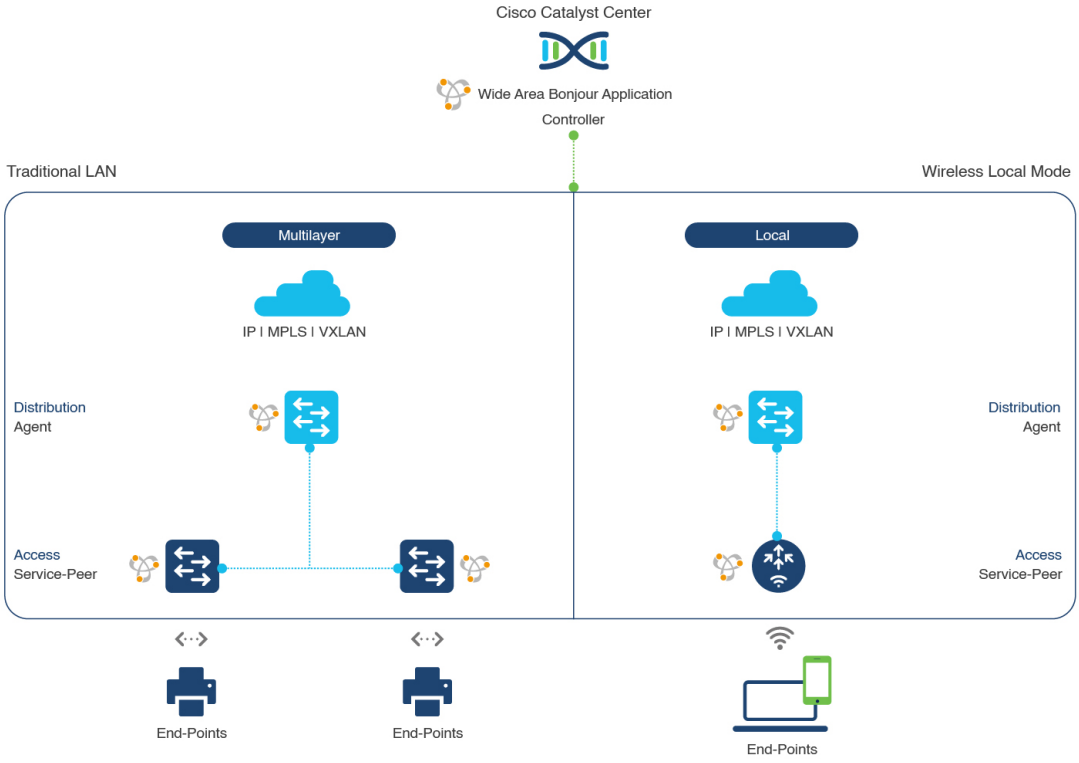
The Cisco DNA Service for Bonjour supports a broad range of enterprise-grade networks. The end-to-end unicast-based Bonjour service routing is supported on traditional, Cisco SD-Access, and BGP EVPN-enabled wired and wireless networks.

Traditional Wired and Wireless Networks

Traditional networks are classic Layer 2 or Layer 3 networks for wired and wireless modes deployed in enterprise networks. Cisco DNA Service for Bonjour supports a broad range of network designs to enable end-to-end service routing and replace flood-n-learn-based deployment with a unicast mode-based solution.

The following figure illustrates traditional LAN and central-switching wireless local mode network designs that are commonly deployed in an enterprise.

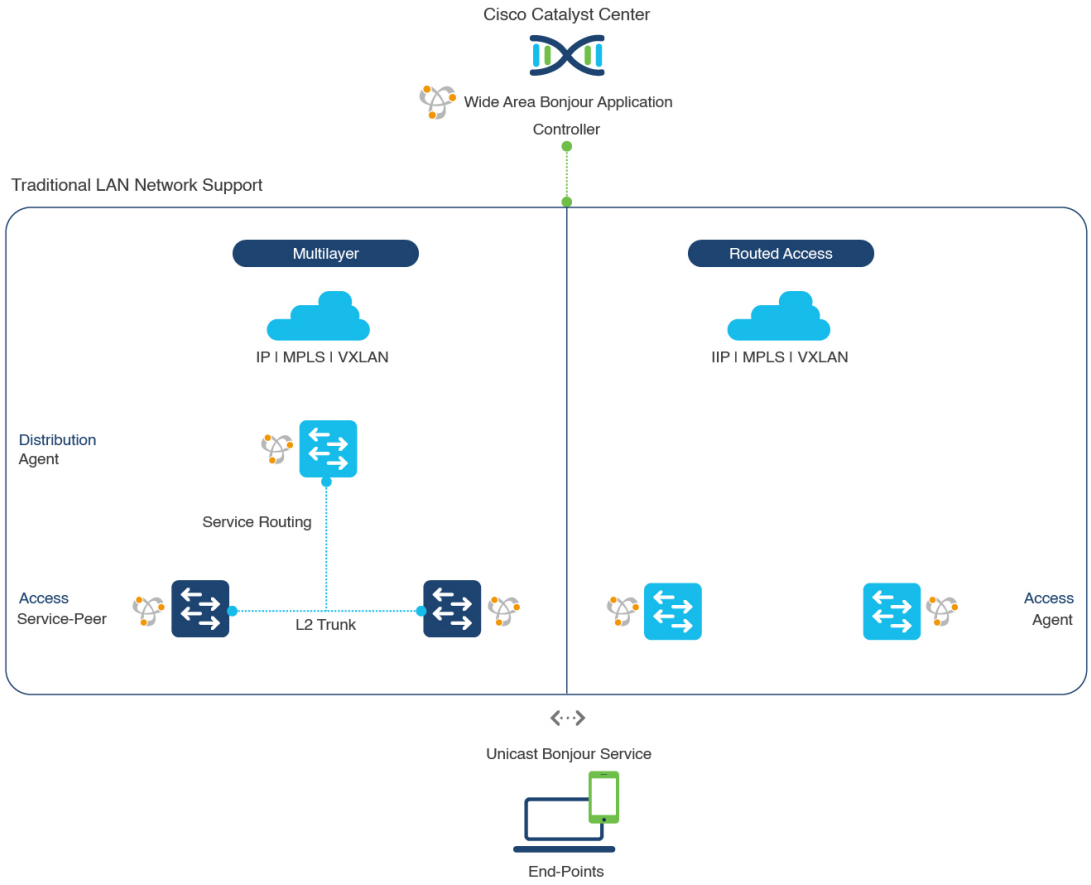
Figure 60: Enterprise Traditional LAN and Wireless Local Mode Network Design



Wired Networks

The following figure shows the supported traditional LAN network designs that are commonly deployed in an enterprise.

Figure 61: Enterprise Wired Multilayer and Routed Access Network Design



The Cisco Catalyst or Cisco Nexus 9300 Series Switches in SDG agent role that provide Bonjour gateway functions are typically IP gateways for wired endpoints that could reside in the distribution layer in multilayer network designs, or in the access layer in Layer 3 routed access network designs:

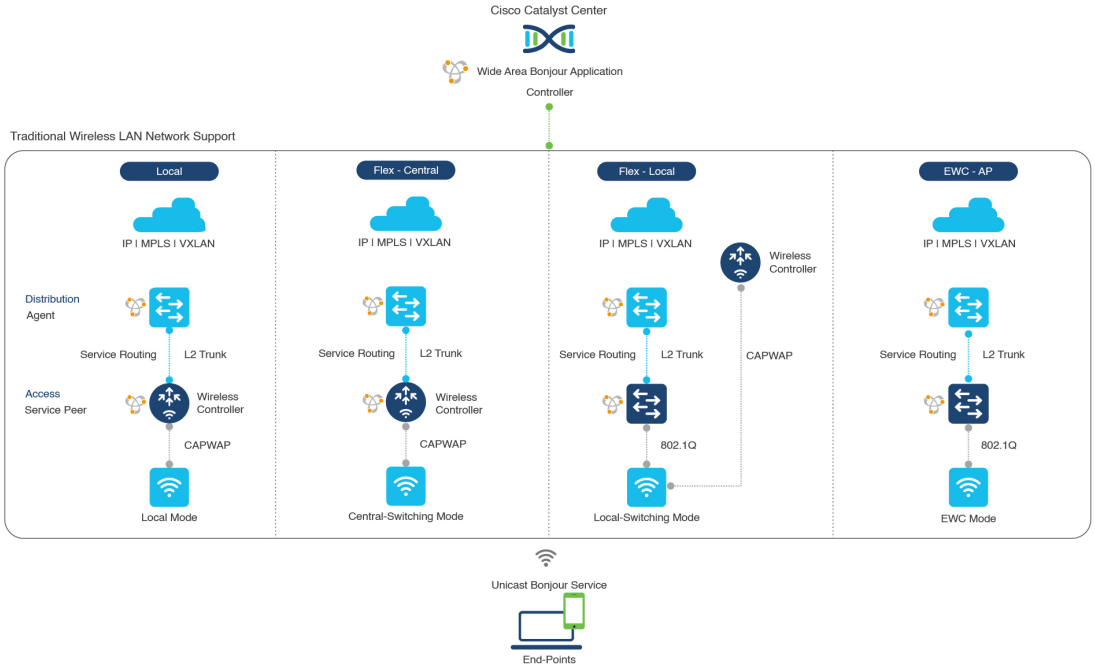
- **Multilayer LAN—Unicast Mode**: In this deployment mode, the Layer 2 access switch provides the first-hop mDNS gateway function to locally attached wired endpoints. In unicast mode, the mDNS services are routed to the distribution layer systems providing IP gateway and SDG agent mode. The policy-based service routing between the SDG agents is performed by the Catalyst Center controller.
- **Multilayer LAN—Flood-n-Learn Mode**: In this deployment mode, the Layer 2 access switch or wireless controller are in mDNS passthrough modes with the Cisco Catalyst or Cisco Nexus 9300 Series Switches operating in the SDG agent mode. The mDNS gateway function at distribution layer in a network enables inter-VLAN mDNS local proxy. It also builds stateful Wide Area Bonjour unicast service routing with the Catalyst Center to discover or distribute mDNS services beyond a single IP gateway.
- **Routed Access**: In this deployment mode, the first-hop Cisco Catalyst or Cisco Nexus 9300 Series Switch is an IP gateway boundary and, therefore, it must also perform the SDG agent role. The policy-based service routing between the SDG agents is performed by the Catalyst Center controller.

Wireless Networks

The Cisco DNA Service for Bonjour extends the single wireless controller mDNS gateway function into the Wide Area Bonjour solution. The mDNS gateway on Cisco Catalyst 9800 Series Wireless Controller can be deployed in an enhanced mode as a service peer. In this mode, the wireless controller builds unicast service routing with an upstream Cisco Catalyst gateway switch for end-to-end mDNS service discovery. It replaces the classic flood-n-learn mDNS services from wired network using mDNS AP or other methods.

The following figure shows the supported traditional wireless LAN network designs that are commonly deployed in an enterprise. Based on the wireless network design, the mDNS gateway function may be on the wireless controller, or first-hop Layer 2 or Layer 3 Ethernet switch of an Access Point in local-switching mode.

Figure 62: Enterprise Traditional Wireless LAN Network Design



The Cisco DNA Service for Bonjour supports the following modes for wireless LAN networks:

- **Local Mode**: In the central switching wireless deployment mode, the m-DNS traffic from local mode Cisco access points is terminated on the Cisco Catalyst 9800 Series Wireless Controller. The Cisco Catalyst 9800 Series Wireless Controller extends the mDNS gateway function to the new service peer mode. The wireless controller can discover and distribute services to local wireless users and perform unicast service routing over a wireless management interface to the upstream Cisco Catalyst Switch in the distribution layer, which acts as the IP gateway and the SDG agent.
- **FlexConnect—Central**: The mDNS gateway function for Cisco access point in FlexConnect central switch SSID functions consistently as described in **Local Mode**. The new extended mDNS gateway mode on the Cisco Wireless Controller and upstream service routing with SDG agent operate consistently to discover services across network based on policies and locations.
- **FlexConnect—Local**: In FlexConnect local switching mode, the Layer 2 access switch in mDNS gateway service peer mode provides the policy-based mDNS gateway function to locally attached wired and wireless users. The Cisco Catalyst Switches in the distribution layer function as SDG agents and enable

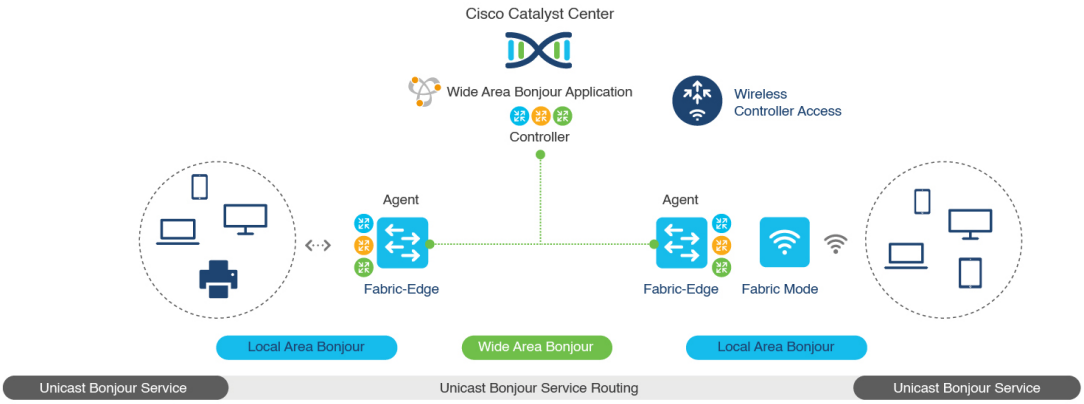
mDNS service-routing across all Layer 2 ethernet switches to support unicast-based service routing to LAN and wireless LAN user groups.

- **Embedded Wireless Controller—Access Point**: The Layer 2 access switch in service peer mode provides unified mDNS gateway function to wired and wireless endpoints associated with Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Series Access Points. The SDG agent in the distribution layer provides unicast service routing across all Layer 2 service peer switches in the Layer 2 network block without any mDNS flooding.

Cisco SD-Access Wired and Wireless Networks

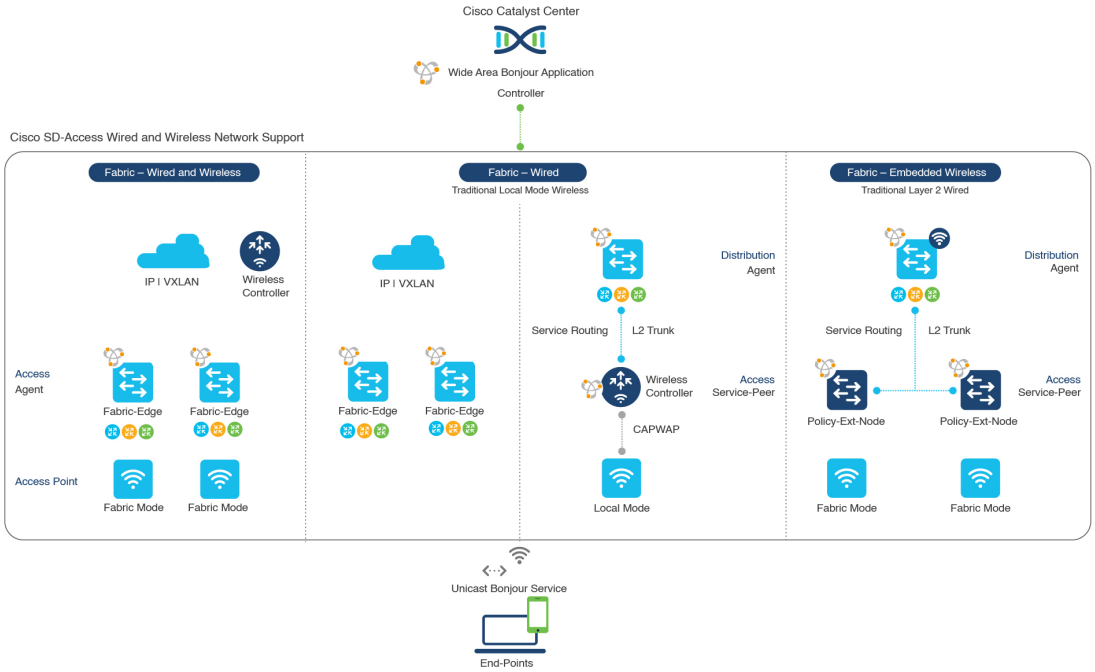
Cisco SD-Access-enabled wired and wireless networks support Cisco DNA Service for Bonjour across fabric networks. The Cisco Catalyst 9000 Series Switches support VRF-aware Wide Area Bonjour service routing to provide secure and segmented mDNS service discovery and distribution management for virtual networks. The VRF-aware unicast service routing eliminates the need to extend Layer 2 flooding, and improves the scale and performance of the fabric core network and endpoints.

Figure 63: Cisco SD-Access Wired and Wireless Network Design



Cisco SD-Access supports flexible wired and wireless network design alternatives to manage fully distributed, integrated, and backward-compatible traditional network infrastructure. Wide Area Bonjour service routing is supported in all network designs providing intuitive user experience. The following figure illustrates the various SD-Access enabled wired and wireless network design alternatives.

Figure 64: Cisco SD-Access Wired and Wireless Network Design Alternatives



The Cisco DNA Service for Bonjour for SD-Access enabled wired and fabric, or traditional mode-wireless networks use two-tier service routing providing end-to-end unicast-based mDNS solution. Based on the network design, each solution component is enabled in a unique role to support the Wide Area Bonjour domain:

- **Fabric Edge SDG Agent**: The Layer 3 Cisco Catalyst Fabric Edge switch in the access layer configured as SDG agent provides unicast-based mDNS gateway function to the locally attached wired and wireless endpoints. The VRF-aware mDNS service policy provides network service security and segmentation in a virtual network environment. The mDNS services can be locally distributed and routed through centralized Catalyst Center.
- **Policy Extended Node**: The Layer 2 Cisco Catalyst access layer switch enables first-hop mDNS gateway function without flooding across the Layer 2 broadcast domain. The unicast-based service routing with upstream Fabric Edge switch in the distribution layer enables mDNS service routing within the same Layer 2 network block. It can also perform remote service discovery and distribution from centralized Catalyst Center.
- **Cisco Wireless Controller**: Based on the following wireless deployment modes, Cisco Wireless Controller supports unique function to enable mDNS service routing in Cisco SD-Access enabled network:
  - **Fabric-Enabled Wireless**: Cisco Wireless Controller doesn't require any mDNS gateway capability to be enabled in distributed fabric-enabled wireless deployments.
  - **Local Mode Wireless**: As Cisco Wireless Controller provides central control and data plane termination, it provides mDNS gateway in service peer mode for wireless endpoints. The wireless controller provides mDNS gateway between locally associated wireless clients. The wireless controller builds service routing with upstream SDG agent Catalyst switch providing IP gateway and service routing function for wireless endpoints.
  - **Embedded Wireless Controller—Switch**: The Cisco Embedded Wireless Controller solution enables the lightweight integrated wireless controller function within the Cisco Catalyst 9300 Series

Switch. The Cisco Catalyst switches in the distribution layer function as SDG agents to the wired and wireless endpoints. The SDG agent in the distribution layer provides unicast service routing across all wireless access points and Layer 2 service peer switches without mDNS flooding.

- **Catalyst Center Controller**: The Cisco Wide Area Bonjour application on Catalyst Center supports policy and location-based service discovery, and distribution between network-wide distributed Fabric Edge switches in SDG agent mode.

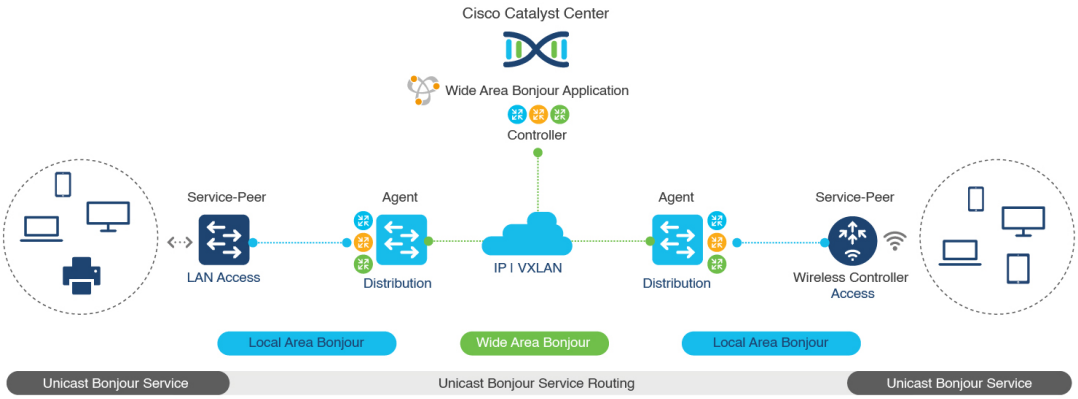
The Wide Area Bonjour communication between the SDG agent and controller takes place through the network underlay. Based on policies, the SDG agent forwards the endpoint announcements or queries to the Catalyst Center. After discovering a service, the endpoints can establish direct unicast communication through the fabric overlay in the same virtual network. The inter-virtual network unicast communication takes place through the Fusion router or external Firewall system. This communication is subject to the configured overlay IP routing and Security Group Tag (SGT) policies.

BGP EVPN Networks

The BGP EVPN-based technology provides a flexible Layer 3 segmentation and Layer 2 extension overlay network. The VRF and EVPN VXLAN-aware Wide Area Bonjour service routing provides secure and segmented mDNS service solution. The overlay networks eliminate mDNS flooding over EVPN-enabled Layer 2 extended networks and solve the service reachability challenges for Layer 3 segmented routed networks in the fabric.

The following figure shows the BGP EVPN leaf switch in the distribution layer, supporting overlay Bonjour service routing for a BGP EVPN-enabled traditional Layer 2 wired access switch and traditional wireless local mode enterprise network interconnected through various types of Layer 2 networks and Layer 3 segmented VRF-enabled networks.

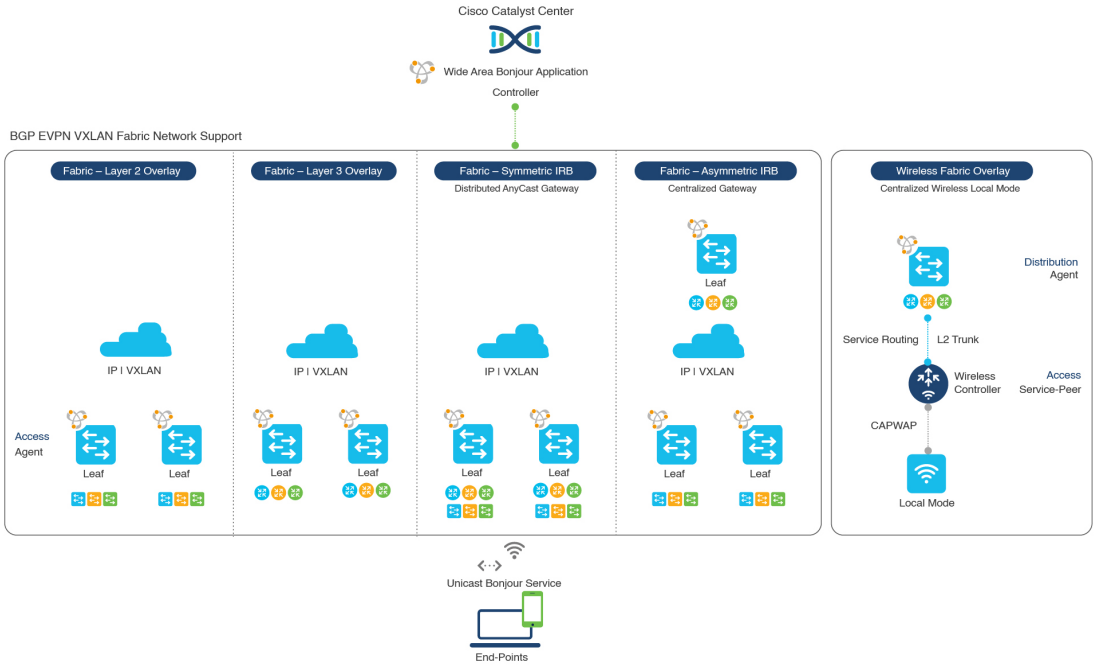
Figure 65: Overlay Bonjour Service for a BGP EVPN-Enabled Enterprise Network



Cisco DNA Service for Bonjour supports all the industry-standard overlay network designs enabling end-to-end unicast-based mDNS service routing, and preventing flooding and service boundary limitation across wired and wireless networks.

The following figure illustrates the various BGP EVPN VXLAN reference overlay network design alternatives. This network design enables end-to-end mDNS service discovery and distribution based on overlay network policies.

Figure 66: BGP EVPN VXLAN Wired and Wireless Design Alternatives



The Cisco Catalyst and Cisco Nexus 9000 Series Switches can be deployed in Layer 2 or Layer 3 leaf roles supporting mDNS service routing for a broad range of overlay networks. In any role, the mDNS communication is limited locally and supports end-to-end unicast-based service routing across Wide Area Bonjour domain:

- **Layer 2 Leaf SDG Agent**: The Cisco Catalyst or Cisco Nexus switches can be deployed as Layer 2 leaf supporting end-to-end bridged network with IP gateway within or beyond BGP EVPN VXLAN fabric network. By default, the mDNS is flooded as Broadcast, Unknown Unicast, Multicast (BUM) over the fabric-enabled core network. This mDNS flooding may impact network performance and security. The Layer 2 leaf, enabled as SDG agent, prevents mDNS flooding over VXLAN and supports unicast-based service routing.
- **Layer 3 Leaf SDG Agent**: The Cisco Catalyst or Cisco Nexus switches can be deployed as SDG agent supporting Layer 3 overlay network in BGP EVPN VXLAN fabric. The IP gateway and mDNS service boundary is terminated at the SDG agent switches and remote services can be discovered or distributed through centralized Catalyst Center.
- **Local Mode Wireless**: The centralized wireless local mode network can be terminated within or outside the EVPN VXLAN fabric domain to retain network segmentation and service discovery for wireless endpoints. The Cisco Catalyst 9800 Series Wireless Controller in service peer mode can build unicast service routing with distribution layer IP and SDG agent Cisco Catalyst switch to discover services from BGP EVPN VXLAN fabric overlay network.
- **Catalyst Center**: Catalyst Center supports Wide Area Bonjour capability to dynamically discover and distribute mDNS services based on Layer 2 or Layer 3 Virtual Network ID (VNID) policies to route the mDNS services between SDG agent switches in the network.

For more information about BGP EVPN networks, see *Cisco DNA Service for Bonjour Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9600 Switches)*.

CHAPTER 192

Configuring Local and Wide Area Bonjour Domains

- Cisco DNA Service for Bonjour Solution Overview, on page 2159
- Configuring Local and Wide Area Bonjour Domains, on page 2171
- Configuring Hot Standby Router Protocol-aware (HSRP-aware) mDNS Service-Routing on SDG, on page 2191
- Configuring Hot Standby Router Protocol-aware (HSRP-aware) mDNS Service-Routing on Service-Peer (CLI), on page 2191
- Verifying Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks, on page 2192
- Additional References for DNA Service for Bonjour, on page 2197
- Feature History for Cisco DNA Service for Bonjour, on page 2197

Cisco DNA Service for Bonjour Solution Overview

Restrictions

- Cisco Service Discovery Gateway (SDG) and Wide Area Bonjour gateway function is supported on Cisco Catalyst Switch and Cisco ISR 4000 series routers. See Solution Components, on page 2148 for the complete list of supporting platforms, software versions and license levels.
- Cisco IOS supports classic and new method of building local Bonjour configuration policies. The classic method is based on **service-list mdns-sd** CLI whereas the new method is based on **mdns-sd gateway**. We recommend using the new **mdns-sd gateway** method since the classic configuration support will be deprecated in near future releases.
- The classic to new method CLI migration is manual procedure to convert the configuration.
- The Bonjour service policies on Cisco SDG Gateways are effective between local VLANs. In addition to these, a specific egress policy controls the type of services to be exported to the controller. The Layer 2 Multicast-DNS Bonjour communication between two end-points on same broadcast domain is transparent to gateway.
- To enable end-to-end Wide Area Bonjour solution on Wireless networks, the Cisco WLC controller must not enable mDNS Snooping function. The upstream IP gateway on the dedicated Cisco Catalyst switch must have the Bonjour gateway function enabled for wireless clients.

- Cisco Wireless LAN Controller must enable AP Multicast with unique Multicast group. Without AP joining WLC Multicast group the mDNS messages will not be processed between client and gateway switch. Multicast on Client SSID or VLAN is optional for other multicast applications and not mandatory or required for Bonjour solution.
- Cisco Catalyst 9800 WLC can be configured as mDNS Gateway. In this mode, the Cisco Catalyst 9800 WLC supports Local-Area Bonjour gateway solution limited to Wireless only networks. Cisco Catalyst 9800 does not support Wide Area Bonjour. For end-to-end Wired and Wireless Bonjour support, we recommend using upstream Cisco Catalyst Switch as IP and Bonjour gateway.

Cisco Wide Area Bonjour Service Workflow

The Cisco Wide Area Bonjour solution follows a client-server model. The SDG Agent functions as a client and the Cisco Wide Area Bonjour application Cisco Catalyst Center functions as a server.

The following sections describe the workflow of service announcement and discovery in the IP network.

Announcing Services to the Network

- The endpoint devices (Source) in the Local Area Bonjour domain send service announcements to the SDG Agent and specify what services they offer. For example, _airplay._tcp.local, _raop._tcp.local, _ipp._tcp.local, and so on.
- The SDG Agent listens to these announcements and matches them against the configured Local Area SDG Agent policies. If the announcement matches the configured policies, the SDG Agent accepts the service announcement and routes the service to the controller.

Discovering Services Available in the Network

- The endpoint device (Receiver) connected to the Local Area SDG Agent sends a Bonjour query to discover the services available, using the mDNS protocol.
- If the query conforms to configured policies, SDG Agent responds with the services obtained from appropriate service routing via the Wide Area Bonjour Controller.

Wide Area Bonjour Multi-Tier Policies

The various policies that can be used to control the Bonjour announcements and queries are classified as the following:

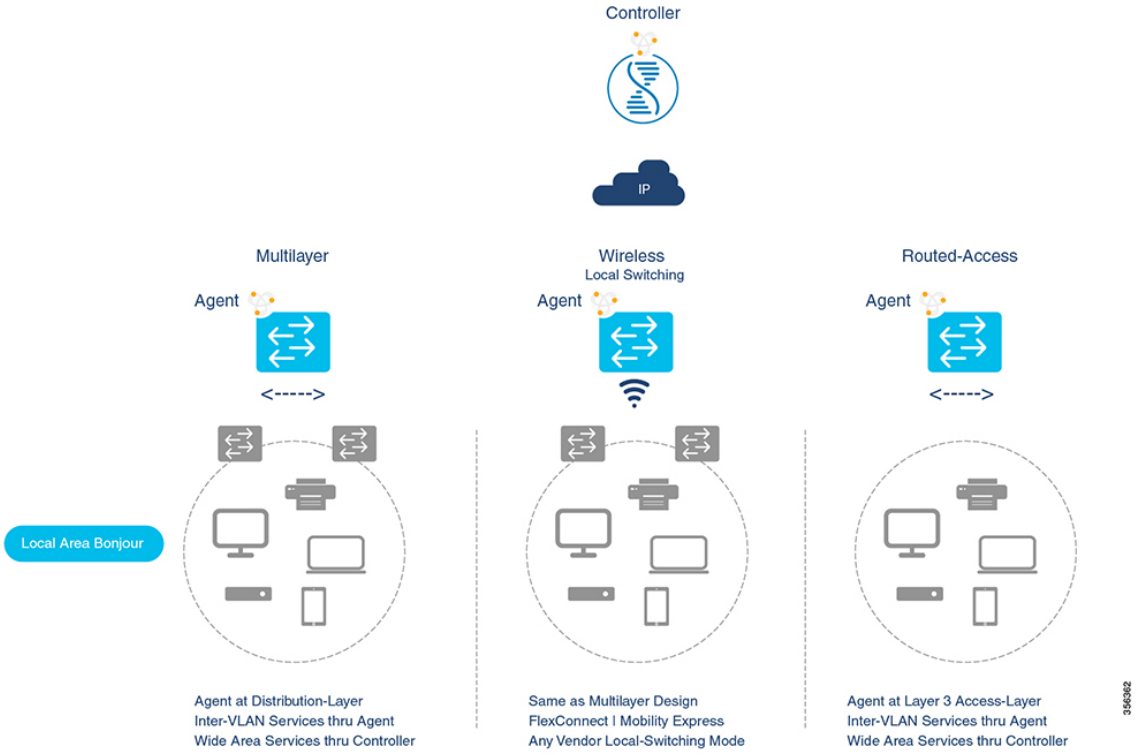
- **Local Area SDG Agent Filters**: Enforced on the SDG Agent in Layer-2 Network Domain. These bi-directional policies control the Bonjour announcements or queries between the SDG Agents and the Bonjour endpoints.
- **Wide Area SDG Agent Filters**: Enforced on the SDG Agent for export control to the Controller. This egress unidirectional policy controls the service routing from the SDG Agent to the controller.
- **Cisco Wide Area Bonjour Policy**: Enforced on Controller for global service discovery and distribution. Policy enforcement, between the controller and the IP network is bi-directional.

Cisco Wide Area Bonjour Supported Network Design

Traditional Wired and Wireless Networks

The Cisco DNA Service for Bonjour supports various LAN network designs commonly deployed in the enterprise. The SDG Agent providing Bonjour gateway functions is typically an IP gateway for wired end-points that could be residing in the distribution layer in multilayer network designs, or in the access layer in routed access network designs.

The following figure shows various topologies which are explained further in the section.

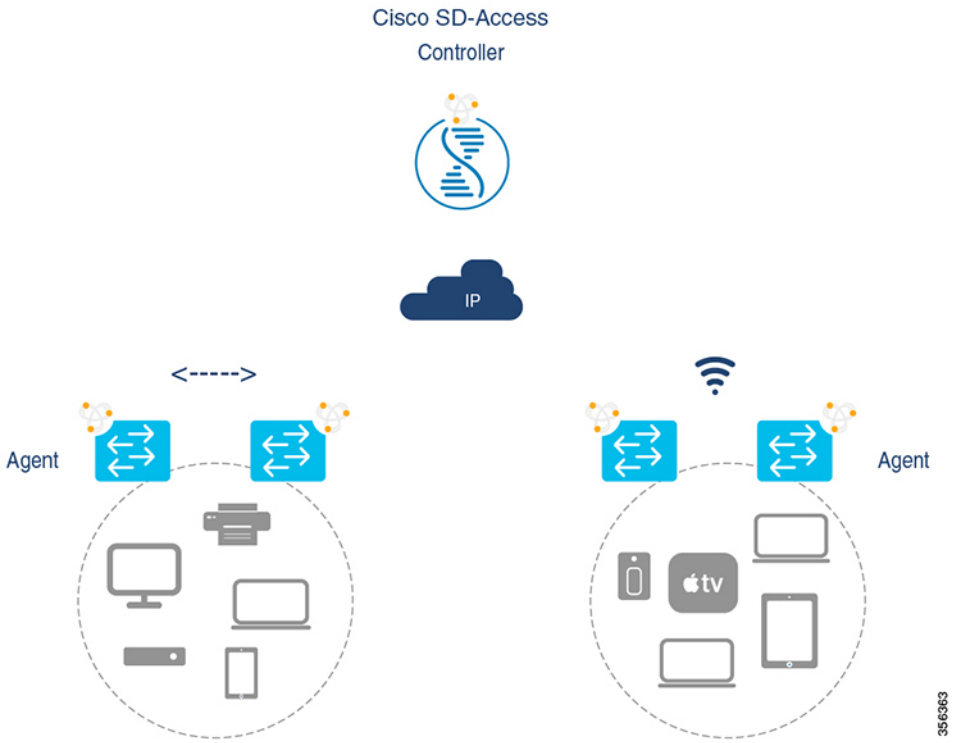


- **Multilayer LAN**: In this deployment mode, the Layer 2 Access switch provides the transparent bridging function of Bonjour services to Distribution-layer systems that act as the IP gateway and SDG Agent. There is no additional configuration or new requirement to modify the existing Layer-2 trunk settings between the Access and Distribution Layer Cisco Catalyst Switches.
- **Routed Access**: In this deployment mode, the first-hop switch is an IP gateway boundary and therefore, it must be combined with the SDG Agent role.

The Cisco DNA Service for Bonjour also supports various Wireless LAN network designs commonly deployed in the Enterprise. The SDG Agent provides consistent Bonjour gateway functions for the wireless endpoints as in wired networks. In general, the IP gateway of the wireless clients is also a Bonjour gateway. However, the placement of the SDG Agent may vary depending on the Wireless LAN deployment mode.

Cisco SD Access Wired and Wireless Networks

In Cisco SD-Access network, the Fabric Edge switch is configured as the SDG Agent for fabric-enabled wired and wireless networks. Wide Area Bonjour policies need to be aligned with the SD-Access network policies with respect to Virtual Networks and SGT policies, if any.



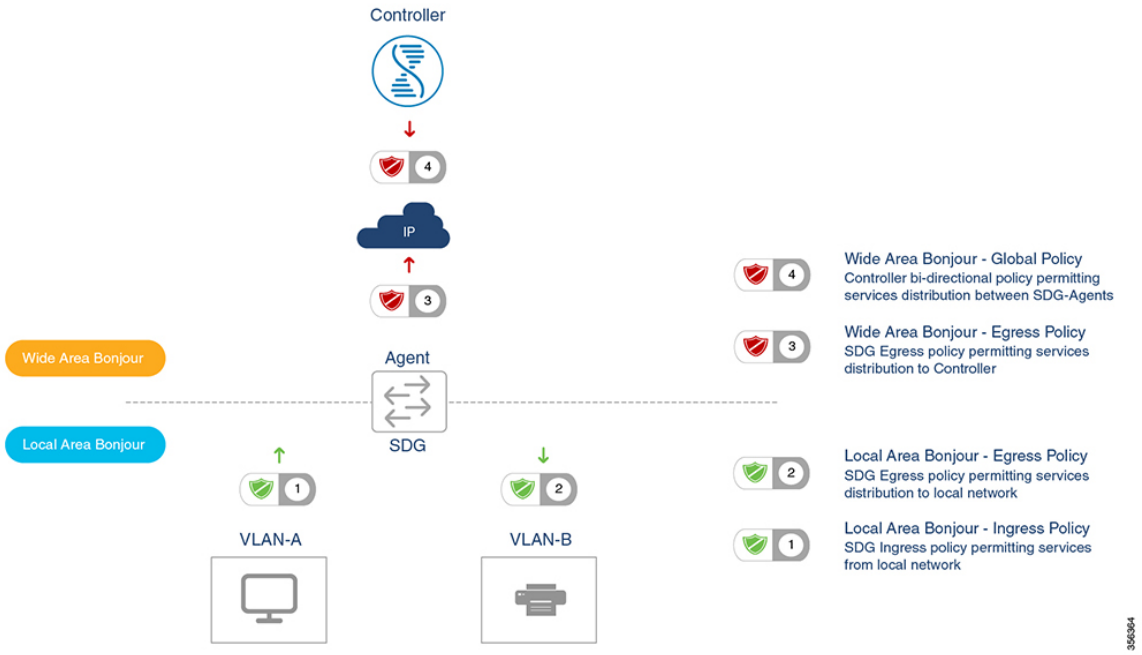
Wide Area Bonjour uses two logical components in a network:

- SDG Agent: The Fabric Edge switch is configured as the SDG Agent, and the configuration is added only after the SD-Access is configured.
- Wide Area Bonjour Controller: The Wide Area Bonjour application in the Cisco Catalyst Center acts as the Controller.

The Wide Area Bonjour communication between the SDG Agent and the Controller takes place through the network underlay. The SDG Agent forwards the endpoint announcements or queries to the Controller through the fabric underlay. After discovering a service, a Bonjour-enabled application establishes direct unicast communication with the discovered device through the fabric overlay. This communication is subject to any configured routing and SDG policies.

Local and Wide Area Bonjour Policies

The Cisco Wide Area Bonjour policy is divided into four unique function to enable policy based Bonjour services discovery and distribution in two-tier domains. The network administrator must identify the list of Bonjour services that needs to be enabled and set the discovery boundary that can be limited to local or global based on requirements. Figure below illustrates enforcement point and direction of all four types of Bonjour policies at the SDG Agent level and in Cisco Catalyst Center Wide Area Bonjour application:

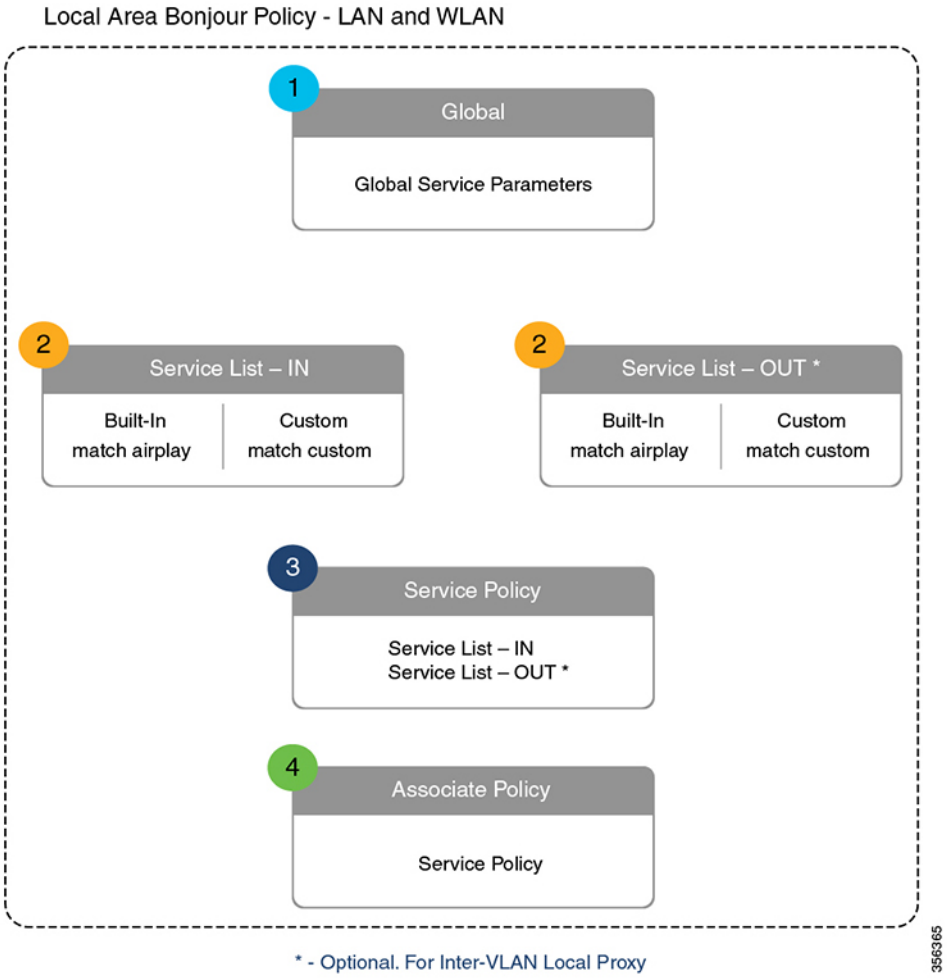


Local Area Bonjour Policy

The Cisco IOS Bonjour policy structure is greatly simplified and scalable with the new configuration mode. The services can be enabled with intuitive user-friendly service-type instead individual mDNS PoinTeR (PTR) records types, for example select AirPlay that automatically enables video and audio service support from Apple TV or equivalent capable devices. Several common types of services in Enterprise can be enabled with built-in service-types. If built-in service type is limited, network administrator can create custom service-type and enable the service distribution in the network.

The policy configuration for the Local Area Bonjour domain is mandatory, and is a three step process. Figure below illustrates the step-by-step procedure to build the Local-Area Bonjour policy, and apply to enable the gateway function on selected local networks:

Figure 67: Local Area Bonjour Policy Hierarchy



To configure local area bonjour policies, enable mDNS globally. For the device to receive mDNS packets on the interface, configure mDNS gateway on the interface. Create a service-list by using filter options within it allow services into or out of a device or interface. After enabling mDNS gateway globally and on the interface, you can apply filters (IN-bound filtering or OUT-bound filtering) on service discovery information by using **service-policy** commands.

Built-In Service List

The Cisco IOS software includes built-in list of services that may consist of one more Bonjour service-type. A single service-list may contain more than one service-type entries with default rule to accept service announcement from service-provider and the service query request from receiver end-points. If selected service-type contains more than one Bonjour service-types (PTR), then a service announcement or a service query is honored when the announcement/query is for any one of these included Bonjour service-types. For example, Apple Time Capsule Data service-type consists of both_adisk and _afpovertcp built-in PTRs, however if any end-point announces or requests for only _afpovertcp service, then SDG Agent will successfully classify and process the announcement or request. The service-list contains implicit-deny for all un-defined built-in or custom services entries.

Table below illustrates complete list of built-in Bonjour services that can be used to create policies in local area Bonjour.

Table 147: Cisco IOS Built-In Bonjour Service Database

Service	Service Name	mDNS PTRs
Airplay	airplay	_airplay._tcp.local
Apple TV	apple-tv	_airplay._tcp.local _raop._tcp.local
Audinate	audinate	_dante-safe._udp.local _dante-upgr._udp.local _netaudio-arc._udp.local _netaudio-chan._udp.local _netaudio-cmc._udp.local _netaudio-dbc._udp.local
AirServer Mirroring Service	airserver	_airplay._tcp.local _airserver._tcp.local
Apple AirTunes	airtunes	_raop._tcp.local
Amazon Fire TV	amazon-fire-tv	_amzn-wplay._tcp.local
Apple AirPrint	apple-airprint	_ipp._tcp.local _universal._sub._ipp._tcp.local
Apple TV 2	apple-continuity	_companion-link._tcp.local
Apple File Share	apple-file-share	_afpovertcp._tcp.local
Apple HomeKit	apple-homekit	_homekit._ipp.local _hap._tcp.local
Apple iTunes Library	apple-itunes-library	_atc._tcp.local
Apple iTunes Music	apple-itunes-music	_daap._tcp.local
Apple iTunes Photo	apple-itunes-photo	_dpap._tcp.local
Apple KeyNote Remote Control	apple-keynote	_keynotecontrol._tcp.local _keynotepair._tcp.local
Apple Remote Desktop	apple-rdp	_afpovertcp._tcp.local _net-assistant._tcp.local
Apple Remote Event	apple-remote-events	_eppc._tcp.local

Service	Service Name	mDNS PTRs
Apple Remote Login	apple-remote-login	_sftp-ssh._tcp.local _ssh._tcp.local
Apple Screen Share	apple-screen-share	_rfb._tcp.local
Google Expeditions	google-expeditions	_googexpeditions._tcp.local
Apple Time Capsule Data	apple-timecapsule	_adisk._tcp.local _afpovertcp._tcp.local
Apple Time Capsule Management	apple-timecapsule-mgmt	_airport._tcp.local
Apple MS Window File Share	apple-windows-fileshare	_smb._tcp.local
Fax	fax	_fax-ipp._tcp.local
Google ChromeCast	google-chromecast	_googlecast._tcp.local _googlerpc._tcp.local _googlezone._tcp.local
Apple HomeSharing	homesharing	_home-sharing._tcp.local
Apple iTunes Data Sync	itune-wireless-devicesharing2	_apple-mobdev2._tcp.local
Multifunction Printer	multifunction-printer	_ipp._tcp.local _scanner._tcp.local _fax-ipp._tcp.local
Phillips Hue Lights	phillips-hue-lights	_hap._tcp.local
Printer – Internet Printing Protocol	printer-ipp	_ipp._tcp.local
Printer – IPP over SSL	printer-ipps	_ipps._tcp.local
Linux Printer – Line Printer Daemon	printer-lpd	_printer._tcp.local
Printer Socket	printer-socket	_pdl-datastream._tcp.local
Roku Media Player	roku	_rsp._tcp.local
Scanner	scanner	_scanner._tcp.local
Spotify Music Service	spotify	_spotify-connect._tcp.local
Web-Server	web-server	_http._tcp.local
WorkStation	workstation	_workstation._tcp.local

Custom Service List

The Custom service list allows network administrator to configure service if built-in Bonjour database does not support specific service or bundled service types. For example, the file-sharing requirement demands to support Apple Filing Protocol (AFP) between macOS users and Server Message Block (SMB) file transfer capability between macOS and Microsoft Windows devices. For such requirements the network administrator can create an custom service list combining AFP (_afpovertcp._tcp.local) and SMB (_smb._tcp.local).

The Service-List provides flexibility to network administrator to combine built-in and custom service definition under single list. There is no restriction on numbers of custom service definitions list and association to single service-list.

Policy Direction

The Local Area Bonjour policy in Cisco IOS provides flexibility to network administrator to construct service policies that can align service announcement and query management in same or different local networks. The service-policies can be tied to either ingress or egress direction to enforce service control in both directions. The following sub-sections provide more details on service policy configuration.

Ingress Service Policy

The ingress service policy is a mandatory configuration element that is used to permit the processing of incoming mDNS service announcement and query requests. Without ingress service policy, the Bonjour gateway function on a targeted Wired or Wireless network is not enabled. The ingress service policy provides flexibility to permit service announcement and query on each user-defined service-types, i.e. permit accepting AirPlay service announcement and query request, but enable Printer service query request only.

Egress Service Policy

The egress service policy is an optional configuration and not required in following two conditions:

- The egress service policy is not applicable in local VLAN where the expected Bonjour end-points are service-provider only, i.e. Service-VLAN network may contain only IT managed service-provider end-points such as Apple TV, Printers etc. as these end-points do not query for other service-types in the network.
- The Wired or Wireless users must receive services only from Wide Area Bonjour domain by Cisco Catalyst Center, and not from other Bonjour end points connected to the same SDG Agent.. The egress service policy configuration is only required when an SDG-Agent must distribute locally discovered Bonjour services information from one VLAN to other. For example, based on ingress service policy the SDG-Agent discovered and cache the AirPrint capable Printer from VLAN-A, if the receiver endpoint in VLAN-B wants to discover Printer information from VLAN-A then the SDG-Agent must have ingress and egress service policy permitting AirPrint service on both VLANs.

Conditional Egress Service Policy

The network administrator can optionally customize the egress service policy to enable conditional service response from sourced from specific VLAN network. For example, based on ingress service policy the SDG-Agent may discover AirPrint capable Printers from VLAN-A and VLAN-C networks. With conditional Local Area Bonjour egress service policy rule, the network administrator may limit distributing Printer information discovered from VLAN-A to the receivers in VLAN-B network and automatically filters VLAN-C Printers. The conditional egress service policy support is optional setting and only applicable on out direction service policy.

Service Status Timer Management

The Bonjour service-provider end-points may announces one or more services in the network combining mDNS records and time-to-live (TTL) service timers for each record. The TTL value provides assurance of end-point availability and serviceability in the network. The SDG Agents ensures that it contains up to date information in its local and updates global services in Controller based on TTL and other events in Local Area Bonjour domain. The network administrator must configure the service status timer where service-provider endpoint discovery is permitted.

Wide Area Bonjour Policy

The SDG-Agent mandatorily requires the controller bound Wide Area Bonjour service export policy to control routing local services and discover remote services from Cisco Catalyst Center. As the Cisco Catalyst Center and SDG-Agent builds trusted communication channel the remote service response from Wide Area Bonjour App is implicitly permitted at SDG-Agent. Hence the Wide Area Bonjour policy is unidirectional it only requires egress service policy towards controller.

The Wide Area Bonjour policy hierarchy and structure is identical as described in Local Area Bonjour Policy structure section. Following sub-section provides step-by-step reference configuration to build and enforce the policy to enable the successful communication with Wide Area Bonjour App in Cisco Catalyst Center.

Service List – Built-In and Custom

The network administrator must create new controller bound egress service list for the Wide Area Bonjour domain. In most common network deployment model, the Wide Area Bonjour service list may contain same service-types as the Local Area Bonjour to implement common services between both domains. Based on requirements, certain services can be limited to Local Area and prevent routed in Wide Area Domain, then by default only allowed service list entries are permitted and rest are dropped with implicit deny rule.

Ingress Policy Direction

The ingress service policy for Wide Area Bonjour domain is not required and cannot be associated to the controller.

Egress Policy Direction

As described the Bonjour policy structure between Local Area and Wide Area is consistent, however the enforcement point is different. We recommend configuring separate Service-List and Service-Policy for Wide Area Bonjour domain as it may help building unique policy set for each domain.

Conditional Egress Service List

The Wide Area Bonjour egress service list configuration can be customized to conditionally route the service or query request to the Cisco Catalyst Center. With this alternative configuration settings, the network administrator can route the service or query the request in Wide Area Bonjour domain from specific local source VLAN network instead globally from entire system.

Wide Area Bonjour Service Status Timer Management

The Cisco Catalyst Center centralizes the services information from large scale distributed SDG-Agents across the network. To maintain a scale and performance of controller the services routing information is transmitted and synchronized periodically by each SDG-Agent network devices. To protect system and network performance the scheduler base service information exchange allows graceful and reliable way to discover and distribute Bonjour services across Wide Area Bonjour domain.

In most large-scale network environment, the default Bonjour service timers on SDG-Agents are by default fine-tuned and may not need any further adjustments. Cisco recommends retaining the interval timer values to default and adjust only based on any user experience issue and consider modified parameters do not introduce scale and performance impact.

Default mDNS Service Configurations

Starting with Cisco IOS XE Bengaluru 17.6.1, an intuitive approach to configuring mDNS services, known as the default mDNS service configuration is introduced. The default service configuration contains a default service policy that creates a service list with default service-types that is automatically enforced in the ingress or egress direction. The following figure illustrates the default mDNS service configurations:

Figure 68: Default mDNS Service Configurations

The default mDNS service configurations accelerates solution adoption, increases user productivity, and reduces operation overhead. Additionally, you can define a custom policy and service list with custom-defined service types, and enfore it in the ingress or degress direction.

HSRP-Aware mDNS Service-Routing

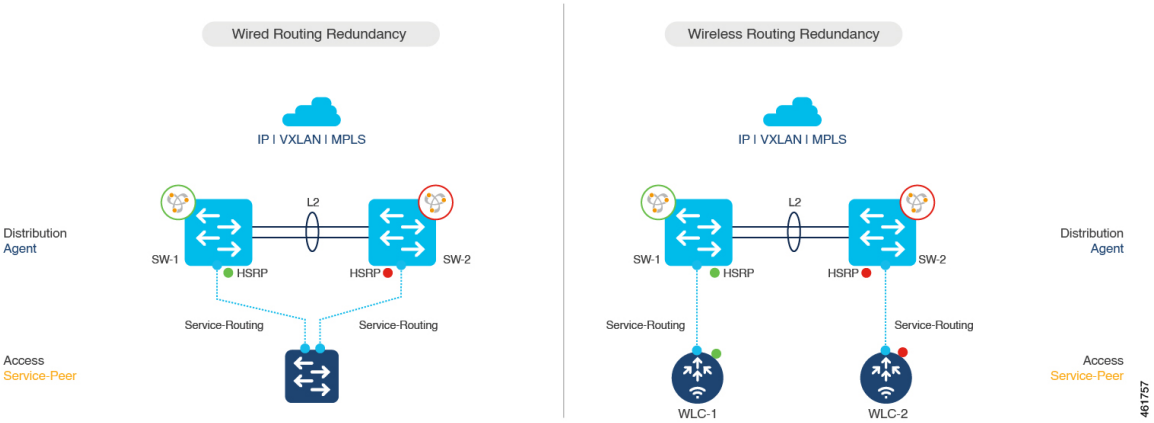
Starting from Cisco IOS XE Bengaluru 17.6.1, Hot Standby Router Protocol-aware (HSRP-aware) mDNS Service-Routing is supported between Service Peers and SDG agents in a multilayer network. During a changeover, that is when the primary SDG agent fails and the secondary SDG agent becomes the new primary, the service-routing session between the Service Peer and the SDG agent remains uninterrupted. The new primary SDG agent establishes a session with the Service Peer and cache information is resynced.

The HSRP virtual IP address of the management VLAN is enabled on the SDG agent using the **standby** *group_number* **ip** *ip_address* command. The HSRP virtual IP address needs to configured on the Service Peer as the IP address of the SDG agent.

Note The HSRP virtual IP address must be reachable and in active state during a changeover.

The following figure illustrates a wired and wireless network that supports HSRP-aware mDNS Service-Routing:

Figure 69: HSRP-Aware mDNS Service-Routing



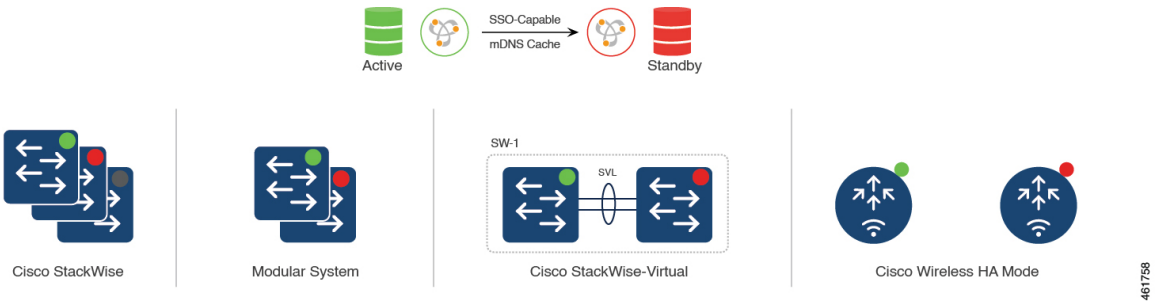
The HSRP offers the following advantages:

- Automatic gateway selection.
- Rapid switchover.
- Reduces service convergence.

mDNS Service-Gateway SSO Support

Starting from Cisco IOS XE Bengaluru 17.6.1, mDNS Stateful Switchover (SSO) is supported on network devices configured in Service Peer role. In SSO-enabled devices, one device is selected as an active device and the other as a standby device. The cache information learnt by the active device is synced with the standby device. When the active device fails, the standby device becomes the new active device and continues the mDNS service discovery process.

Figure 70: mDNS Service-Gateway SSO



Configuring Local and Wide Area Bonjour Domains

How to configure Multicast DNS Mode for LAN and Wired Networks

This section provides information about how to configure Local Area Bonjour in multicast DNS mode.

Enabling mDNS Gateway on the Device

To configure mDNS on the device, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS on the device and enters mDNS gateway configuration mode. Enter the following commands in mDNS gateway configuration mode to enable the respective functionalities: • **air-print-helper**: Enables IOS devices like iPADs to discover and use older printers that support Bonjour • **cache-memory-max**: Configures the percentage memory for cache • **ingress-client**: Configures Ingress Client Packet Tuners • **rate-limit**: Enables rate limiting of incoming mDNS packets • **service-announcement-count**: Configures maximum service advertisement count • **service-announcement-timer**: Configures advertisements announce timer periodicity • **service-query-count**: Configures maximum query count

	Command or Action	Purpose
		• **service-query-timer**: Configures query forward timer periodicity The following CLIs are effective only in service-peer mode: • **query-response** • **sdg-agent** • **service-announcement-count** • **service-announcement-timer** • **service-mdns-query** • **service-query-count** • **service-query-timer** • **service-receiver-purge** • **active-response** **Note** For **cache-memory-max**, **ingress-client**, **rate-limit**, **service-announcement-count**, **service-announcement-timer**, **service-query-count**, and **service-query-timer** commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.
Step 4	**exit** **Example:** `Device(config-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

Creating Custom Service Definition (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS** > **Service Policy** > **Service Definition**.

Step 2 Click **Add**.

Step 3 Enter the **Service Definition Name** and **Description**.

Step 4 Enter the **Service Type** and click the + icon.

Step 5 Click **Apply to Device**.

Creating Custom Service Definition

Service definition is a construct that provides an admin friendly name to one or more mDNS service types or PTR Resource Record Name. By default, a few built-in service definitions are already predefined and available for admin to use. In addition to built-in service definitions, admin can also define custom service definitions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition CUSTOM1`	Configures mDNS service definition. **Note** All the created custom service definitions are added to the primary service list. Primary service list comprises of a list of custom and built-in service definitions.
Step 4	**service-type** *string* **Example:** `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	Configures mDNS service type.
Step 5	Repeat step 4 to configure more than one service type in the custom service definition.	
Step 6	**exit** **Example:** `Device(config-mdns-ser-def)# exit`	Exit mDNS service definition configuration mode.

Creating Service List (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS** > **Service Policy** > **Service List**.

Step 2 Click **Add**.

Step 3 Enter the **Service List Name** and choose the direction from the **Direction** drop-down list.

Step 4 Click **Add Service**.

Step 5 Choose the service from the **Available Services** drop-down list and the message type from the **Message Type** drop-down list.

Step 6 Click **Save**.

Step 7 Click **Apply to Device**.

Creating Service List

mDNS service list is a collection of service definitions. To create a service list, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config)# mdns-sd service-list VLAN100-list in`	Configures mDNS service list.
Step 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] **Example:** `Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`	Matches the service to the message type. Here, *service-definition-name* refers to the names of services, such as, airplay, airserver, airtunes, and so on.

	Command or Action	Purpose
		Note To add a service, the service name must be part of the primary service list. If the mDNS service list is set to IN, the applicable command syntax is: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]. If the mDNS service list is set to OUT, the applicable command syntax is: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] [**location-filter** *location-filter-name*] [**source-interface** {*mDNS-VLAN-number* | *mDNS-VLAN-range*}].
Step 5	**exit** **Example:** `Device(config-mdns-sl-in)# exit`	Exits mDNS service list configuration mode.

Creating Service Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS** > **Service Policy** > **Service Policy**.

Step 2 Click **Add**.

Step 3 Enter the **Service Policy Name**.

Step 4 Choose the service list input from the **Service List Input** drop-down list.

Step 5 Choose the service list output from the **Service List Output** drop-down list.

Step 6 Choose the location from the **Location** drop-down list.

Step 7 Click **Apply to Device**.

Creating Service Policy

A Service Policy that is applied to an interface specifies the allowed Bonjour service announcements or the queries of specific service types that should be processed, in ingress direction or egress direction or both. For this, the service policy specifies two service-lists, one each for ingress and egress directions. In the Local Area

Bonjour domain, the same service policy can be attached to one or more Bonjour client VLANs; however, different VLANs may have different service policies.

To configure service policy with service lists, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures mDNS service policy.

Step 4	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config-mdns-ser-pol)# service-list VLAN100-list in`
	`Device(config-mdns-ser-pol)# service-list VLAN300-list out`
		Configures service lists for IN and OUT directions.

Step 5	**exit** **Example:** `Device(config-mdns-ser-pol)# exit`	Exits mDNS service policy configuration mode.

Associating Service Policy to an Interface

To configure mDNS on the device, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *interface-name* **Example:** `Device(config)# interface Vlan 601`	Enters interface mDNS configuration mode and enables interface configuration.
Step 4	**mdns-sd gateway** **Example:** `Device(config-if)# mdns-sd gateway`	Configures mDNS gateway on the interface. Enter the following commands in the interface mDNS gateway configuration mode to enable the respective functionalities: • **active-query**: Sets the time interval for SDG agent to refresh the active status of connected Bonjour client services. The timer value ranges from 60 to 3600 seconds. **Note** This configuration is mandatory only on VLANs whose Bonjour policy is configured to accept Bonjour service announcements from connected Bonjour clients. If the VLAN is configured to only accept Bonjour queries but not Bonjour service announcements, this configuration is optional. • **service-instance-suffix**(Optional) : Appends the service instance suffix to any announced service name that is forwarded to the controller. • **service-mdns-query** [**ptr** | **all**]: Configures mDNS query request message processing for the specified query types. This command is applicable when the controller is in service-peer mode. **Note** By default, the **service-mdns-query** command allows only PTR queries. If you need to respond to all (PTR, SRV, and TXT) queries, you need to execute the following command: **service-mdns-query all** • **service-policy** *policy-name*: Attaches the specified service policy to the VLAN.

	Command or Action	Purpose
		Bonjour announcements, and queries received by and sent from the VLAN are governed by the policies configured in the service policy. This configuration is mandatory for all VLANs. **Note** Service policies can only be attached at interface level. • **transport** [**all** | **ipv4** | **ipv6**] (Optional): Configures BCP parameter. It is recommended to use **transport ipv4** command, except in those networks where the Bonjour clients send only IPv6 announcements and queries.
Step 5	**exit** **Example:** `Device(config-if-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

How to Configure Local Area Bonjour in Multicast DNS Mode for Wireless Networks

The configuration of local area Bonjour on a switch that acts as the SDG Agent in a wireless network involves the same set of procedures that are used to configure local area Bonjour on a switch that acts as the SDG Agent in a wired network.

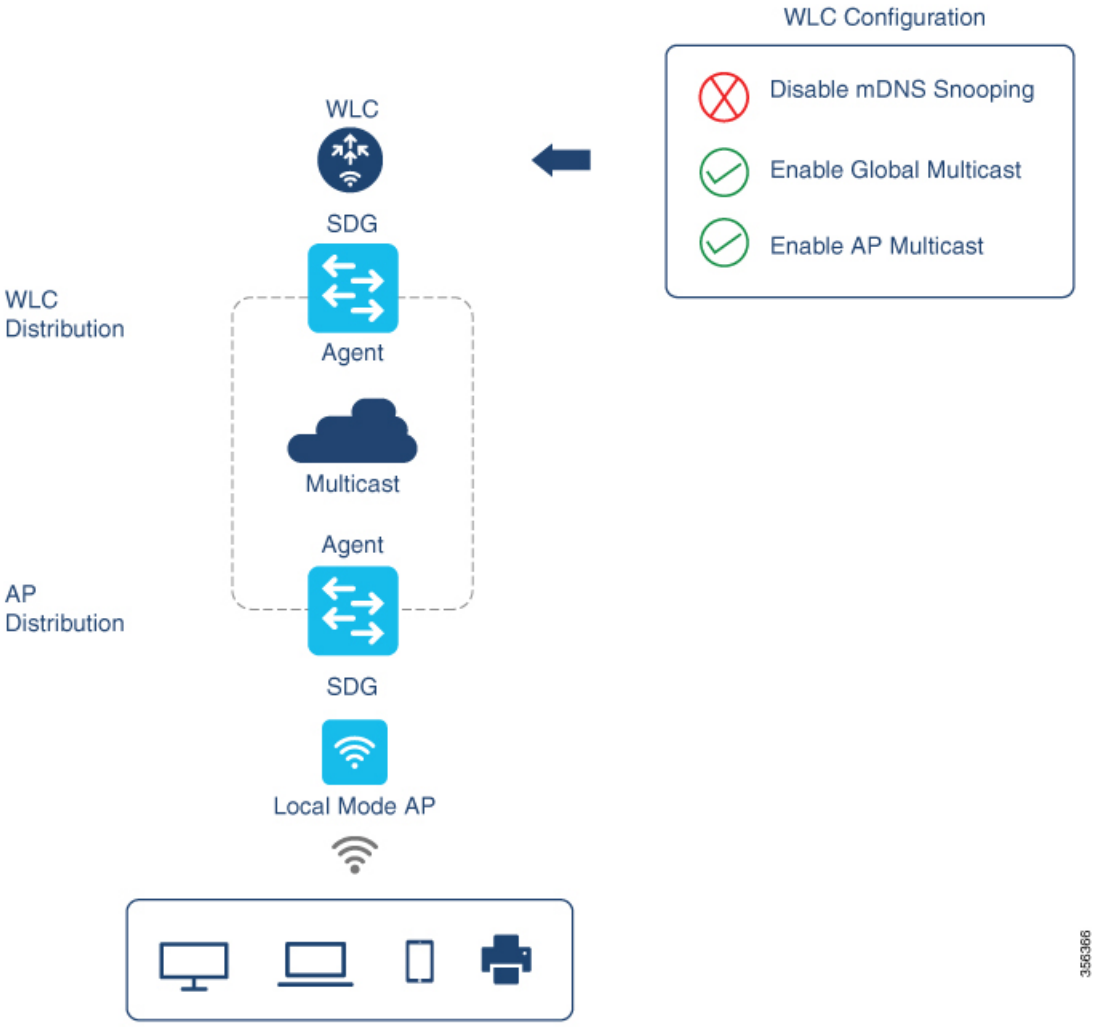
The Bonjour protocol operates on service announcements and queries. Each query or advertisement is sent to the mDNS IPv4 address 224.0.0.251 and IPv6 address FF02::FB. The mDNS messages are carried over well-known industry standard UDP port 5353, over both Layer 3 transport types.

The Layer 2 address used by the Bonjour protocol is link-local multicast address and therefore it's only forwarded to the same Layer 2 network. As multicast DNS (mDNS) is limited to a Layer 2 domain, for a client to discover a service, it has to be a part of the same Layer 2 domain. This isn't always possible in a large-scale deployment or enterprise.

To enable mDNS communication between Wireless endpoints and Cisco Catalyst switch that acts as an SDG Agent, the intermediate WLC must transparently allow the network to transmit and receive mDNS messages.

Hence, for a Multicast DNS Mode Wireless network deployment, disable the mDNS Snooping on Cisco AireOS based WLC and enable mDNS Gateway feature on Cisco Catalyst 9800 series WLC and set the AP Multicast Mode to Multicast.

Figure below illustrates a prerequisite configuration for Wireless network to enable seamless communication between SDG-Agent switches and Wireless endpoints.



The Cisco WLC and Access Points by default prevent the forwarding of Layer 2 or Layer 3 Multicast frames between Wireless and Wired network infrastructure. The forwarding is supported with stateful capabilities enabled using AP Multicast. The network administrator must globally enable Multicast and configure a unique Multicast Group to advertise in the network. This multicast group is only required for Cisco Access Points to enable Multicast over Multicast (MCMC) capabilities across the LAN network. The Bonjour solution doesn't require any Multicast requirements on Wireless Client VLAN; thus, it's optional and applicable only for other Layer 3 Multicast applications.

The core network must be configured with appropriate Multicast routing to allow the Access Points to join WLC Multicast Group. The Multicast configuration must be enabled on Cisco WLC management VLAN and on the Cisco Access Points of their respective distribution layer switch.

Enabling mDNS Gateway on the Device

To configure mDNS on the device, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS on the device and enters mDNS gateway configuration mode. Enter the following commands in mDNS gateway configuration mode to enable the respective functionalities: • **air-print-helper**: Enables IOS devices like iPADs to discover and use older printers that support Bonjour • **cache-memory-max**: Configures the percentage memory for cache • **ingress-client**: Configures Ingress Client Packet Tuners • **rate-limit**: Enables rate limiting of incoming mDNS packets • **service-announcement-count**: Configures maximum service advertisement count • **service-announcement-timer**: Configures advertisements announce timer periodicity • **service-query-count**: Configures maximum query count • **service-query-timer**: Configures query forward timer periodicity The following CLIs are effective only in service-peer mode: • **query-response** • **sdg-agent** • **service-announcement-count** • **service-announcement-timer** • **service-mdns-query**

	Command or Action	Purpose
		• **service-query-count** • **service-query-timer** • **service-receiver-purge** • **active-response** **Note** For **cache-memory-max**, **ingress-client**, **rate-limit**, **service-announcement-count**, **service-announcement-timer**, **service-query-count**, and **service-query-timer** commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.
Step 4	**exit** **Example:** `Device(config-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

Creating Custom Service Definition

Service definition is a construct that provides an admin friendly name to one or more mDNS service types or PTR Resource Record Name. By default, a few built-in service definitions are already predefined and available for admin to use. In addition to built-in service definitions, admin can also define custom service definitions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name*	Configures mDNS service definition.

	Command or Action	Purpose
	Example: `Device(config)# mdns-sd service-definition CUSTOM1`	**Note** All the created custom service definitions are added to the primary service list. Primary service list comprises of a list of custom and built-in service definitions.
Step 4	**service-type** *string* **Example:** `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	Configures mDNS service type.
Step 5	Repeat step 4 to configure more than one service type in the custom service definition.	
Step 6	**exit** **Example:** `Device(config-mdns-ser-def)# exit`	Exit mDNS service definition configuration mode.

Creating Service List

mDNS service list is a collection of service definitions. To create a service list, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config)# mdns-sd service-list VLAN100-list in`	Configures mDNS service list.
Step 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] **Example:** `Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`	Matches the service to the message type. Here, *service-definition-name* refers to the names of services, such as, airplay, airserver, airtunes, and so on.

	Command or Action	Purpose
		Note To add a service, the service name must be part of the primary service list. If the mDNS service list is set to IN, the applicable command syntax is: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]. If the mDNS service list is set to OUT, the applicable command syntax is: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] [**location-filter** *location-filter-name*] [**source-interface** {*mDNS-VLAN-number* | *mDNS-VLAN-range*}].
Step 5	**exit** **Example:** `Device(config-mdns-sl-in)# exit`	Exits mDNS service list configuration mode.

Creating Service Policy

A Service Policy that is applied to an interface specifies the allowed Bonjour service announcements or the queries of specific service types that should be processed, in ingress direction or egress direction or both. For this, the service policy specifies two service-lists, one each for ingress and egress directions. In the Local Area Bonjour domain, the same service policy can be attached to one or more Bonjour client VLANs; however, different VLANs may have different service policies.

To configure service policy with service lists, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures mDNS service policy.

Step 4	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config-mdns-ser-pol)# service-list VLAN100-list in`
	`Device(config-mdns-ser-pol)# service-list VLAN300-list out`
		Configures service lists for IN and OUT directions.

Step 5	**exit** **Example:** `Device(config-mdns-ser-pol)# exit`	Exits mDNS service policy configuration mode.

Associating Service Policy with Wireless Profile Policy

A default mDNS service policy is already attached once the wireless profile policy is created. Use the following steps to override the default mDNS service policy with any of your service policy:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures wireless profile policy.
Step 4	**mdns-sd service-policy** *custom-mdns-service-policy* **Example:** `Device(config-wireless-policy)# mdns-sd service-policy custom-mdns-service-policy`	Associates an mDNS service policy with the wireless profile policy. The default mDNS service policy name is **default-mdns-service-policy**.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-wireless-policy)# exit`	Exits wireless profile policy configuration mode.

Configuring Wide Area Bonjour Domain

The Wide Area Bonjour domain configuration specifies the parameters of the controller, that is the Wide Area Bonjour Application running on Cisco Catalyst Center, as well as the service types that need to be exported to it from the SDG Agent. Configuring Wide Area Bonjour Domain involves creating service-lists and service policy similar to those created in Local Area Bonjour configuration; however, only egress policy from SDG Agent to controller is applicable.

Enabling mDNS Gateway on the Device

To configure mDNS on the device, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS on the device and enters mDNS gateway configuration mode. Enter the following commands in mDNS gateway configuration mode to enable the respective functionalities: • **air-print-helper**: Enables IOS devices like iPADs to discover and use older printers that support Bonjour • **cache-memory-max**: Configures the percentage memory for cache • **ingress-client**: Configures Ingress Client Packet Tuners • **rate-limit**: Enables rate limiting of incoming mDNS packets • **service-announcement-count**: Configures maximum service advertisement count

	Command or Action	Purpose
		• **service-announcement-timer**: Configures advertisements announce timer periodicity • **service-query-count**: Configures maximum query count • **service-query-timer**: Configures query forward timer periodicity The following CLIs are effective only in service-peer mode: • **query-response** • **sdg-agent** • **service-announcement-count** • **service-announcement-timer** • **service-mdns-query** • **service-query-count** • **service-query-timer** • **service-receiver-purge** • **active-response** **Note** For **cache-memory-max**, **ingress-client**, **rate-limit**, **service-announcement-count**, **service-announcement-timer**, **service-query-count**, and **service-query-timer** commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.
Step 4	**exit** **Example:** `Device(config-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

Creating Custom Service Definition

Service definition is a construct that provides an admin friendly name to one or more mDNS service types or PTR Resource Record Name. By default, a few built-in service definitions are already predefined and available for admin to use. In addition to built-in service definitions, admin can also define custom service definitions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition CUSTOM1`	Configures mDNS service definition. **Note** All the created custom service definitions are added to the primary service list. Primary service list comprises of a list of custom and built-in service definitions.
Step 4	**service-type** *string* **Example:** `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	Configures mDNS service type.
Step 5	Repeat step 4 to configure more than one service type in the custom service definition.	
Step 6	**exit** **Example:** `Device(config-mdns-ser-def)# exit`	Exit mDNS service definition configuration mode.

Creating Service List

mDNS service list is a collection of service definitions. To create a service list, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**mdns-sd service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config)# mdns-sd service-list VLAN100-list in`	Configures mDNS service list.
Step 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] **Example:** `Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`	Matches the service to the message type. Here, *service-definition-name* refers to the names of services, such as, airplay, airserver, airtunes, and so on. **Note** To add a service, the service name must be part of the primary service list. If the mDNS service list is set to IN, the applicable command syntax is: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]. If the mDNS service list is set to OUT, the applicable command syntax is: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] [**location-filter** *location-filter-name*] [**source-interface** {*mDNS-VLAN-number* | *mDNS-VLAN-range*}].
Step 5	**exit** **Example:** `Device(config-mdns-sl-in)# exit`	Exits mDNS service list configuration mode.

Creating Service Policy

A Service Policy that is applied to an interface specifies the allowed Bonjour service announcements or the queries of specific service types that should be processed, in ingress direction or egress direction or both. For this, the service policy specifies two service-lists, one each for ingress and egress directions. In the Local Area Bonjour domain, the same service policy can be attached to one or more Bonjour client VLANs; however, different VLANs may have different service policies.

To configure service policy with service lists, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures mDNS service policy.

Step 4	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config-mdns-ser-pol)# service-list VLAN100-list in`
	`Device(config-mdns-ser-pol)# service-list VLAN300-list out`
		Configures service lists for IN and OUT directions.

Step 5	**exit** **Example:** `Device(config-mdns-ser-pol)# exit`	Exits mDNS service policy configuration mode.

Associating Service Policy with the Controller in Wide Area Bonjour Domain

In Wide Area Bonjour, the service policy is configured globally and does not get associated with a VLAN as in the case of Local Area Bonjour.

To configure service policy globally, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**service-export mdns-sd controller** *controller name* **Example:** `Device(config)# service-export mdns-sd controller Cisco Catalyst Center-BONJOUR-CONTROLLER`	Specifies a name for the controller and enters service-export mode
Step 4	**controller-address** *ipv4-address* **Example:** `Device(config-mdns-sd-se)# controller-address 199.245.1.7`	Specifies the controller address.
Step 5	**controller-port** *port-number* **Example:** `Device(config-mdns-sd-se)# controller-port 9991`	Specifies the port number on which the controller is listening.
Step 6	**controller-source-interface** *interface-name* **Example:** `Device(config-mdns-sd-se)# controller-source-interface Loopback0`	Specifies the source-interface for the controller.
Step 7	**controller-service-policy** *service-policy-name* **out** **Example:** `Device(config-mdns-sd-se)# controller-service-policy policy1 OUT`	Specifies the service policy to be used by the controller. **Note** Only OUT policy is applicable for Wide Area Bonjour.
Step 8	**exit** **Example:** `Device(config-mdns-sd)# exit`	Exits controller service export configuration mode.
Step 9	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enters mDNS gateway configuration mode.
Step 10	**ingress-client query-suppression enable** **Example:** `Device(config-mdns-sd)# ingress-client query-suppression enable`	Enables ingress query suppression for better scale and performance.
Step 11	**exit** **Example:** `Device(config-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

Configuring Hot Standby Router Protocol-aware (HSRP-aware) mDNS Service-Routing on SDG

For information, see the following guides:

- Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches)
- Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9400 Switches)
- Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9600 Switches)

Configuring Hot Standby Router Protocol-aware (HSRP-aware) mDNS Service-Routing on Service-Peer (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS on the device and enters mDNS gateway configuration mode.
Step 3	**mode service-peer** **Example:** `Device(config-mdns-sd)# mode service-peer`	Enables mDNS gateway in service-peer mode.
Step 4	**source-interface vlan** vlan-interface-number **Example:** `Device(config-mdns-sd)# source-interface vlan 23`	Configures source interface to communicate between SDG Agent and service-peer. **Note** ***vlan-interface-number***- The valid range is from1 to 4094.
Step 5	**sdg-agent** *ip-address* **Example:** `Device(config-mdns-sd)# sdg-agent 9.6.16.10`	Configures SDG agent IPv4 or IPv6 address. **Note** The *ip-address* refers to the HSRP-enabled IP address.
Step 6	**end** **Example:** `Device(config-mdns-sd)# end`	Exits server group configuration mode and enters privileged EXEC mode.

Verifying Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks

This section shows how to verify Local Area Bonjour in Multicast DNS mode for LAN and Wireless networks.

Verifying SDG-Agent Status

The following is a sample output of the **show mdns-sd service-list** *service-list-name* {**in** | **out**} command.

```
Name           Direction  Service    Message-Type     Source
============================================================
VLAN100-list    In         Printer   Announcement      -
                In         Airplay   Query             -
                In         CUSTOM1   Any               -
VLAN300-list    Out        Printer   Announcement     Vl200
```

The following is a sample output of the **show mdns-sd service-definition***service-definition-name* **service-type** {*custom* | *built-in*} command.

```
Service                PTR                        Type
=========================================================================
apple-tv               _airplay._tcp.local         Built-In
                        _raop._tcp.local
apple-file-share      _afpovertcp._tcp.local      Built-In
CUSTOM1               _custom1._tcp.local         Custom
CUSTOM2               _customA._tcp.local         Custom
                      _customA._tcp.local
```

The following is a sample output of the **show mdns-sd** *service-policy-name* **interface** *interface-name* command.

```
Name   Service-List-In   Service-List-Out
=================================================
mdns-policy-1  VLAN100-list   VLAN300-list
mdns-policy-2  VLAN400-list   VLAN400-list
```

The following is a sample output of the **show mdns-sd summary** command.

```
mDNS Gateway: Enabled
Mode: Service Peer
Service Announcement Periodicity(in seconds): 30
Service Announcement Count: 50
Service Query Periodicity(in seconds): 15
Service Query Count: 50
Active Response Timer (in seconds): Disabled
ANY Query Forward: Disabled
SDG Agent IP: 9.8.57.10
Active Query Periodicity (in minutes): 30
```

```
mDNS Query Type: PTR only
Transport Type: IPv4
mDNS AP service policy: default-mdns-service-policy
```

The following is a sample output of the **show mdns-sd sp-sdg statistics** command.

```
mDNS SP Statistics
last reset time: 07/27/21 15:36:33
Messages sent:
Query : 122
ANY query : 35
Advertisements : 12
Advertisement Withdraw : 1
Service-peer cache clear : 0
Resync response : 3
Srvc Discovery response : 0
Keep-Alive : 2043
Messages received:
Query response : 0
ANY Query response : 0
Cache-sync : 9
Get service-instance : 0
Srvc Discovery request : 0
Keep-Alive Response : 2042
```

Verifying Wide Area Bonjour Controller Status

The following is a sample output of the **show mdns controller summary** command.

```
Device# show mdns controller summary

Controller Summary
====================================
 Controller Name  :   Cisco Catalyst Center-BONJOUR-CONTROLLER
 Controller IP    :   10.104.52.241
 State            :   UP
 Port             :   9991
 Interface        :   Loopback0
 Filter List      :   policy1
 Dead Time        :   00:01:00
```

The following is a sample output of the **show mdns controller export-summary** command.

```
Device# show mdns controller export-summary

Controller Export Summary
=========================
 Controller IP    :   10.104.52.241
 State            :   UP
 Filter List      :   policy1
 Count            :   100
 Delay Timer      :   30 seconds
 Export           :   300
```

```
 Drop             :   0
 Next Export      :   00:00:01
```

The following is a sample output of the **show mdns controller statistics** command.

```
Device# show mdns controller statistics

Total BCP message sent           : 47589
  Total BCP message received       : 3
  Interface WITHDRAW messages sent : 0
  Clear cache messages sent        : 0
  Total RESYNC state count         : 0
  Last successful RESYNC           : Not-Applicable

  Service Advertisements:
   IPv6 advertised                 : 0
   IPv4 advertised                 : 300
   Withdraws sent                  : 0
   Advertisements Filtered         : 0
   Total service resynced          : 0

  Service Queries:
   IPv6 queries sent               : 0
   IPv6 query responses received   : 0
   IPv4 queries sent               : 0
   IPv4 query responses received   : 0
```

The following is a sample output of the **show mdns controller detail** command.

```
Device# show mdns controller detail

Controller : Cisco Catalyst Center-BONJOUR-CONTROLLER
 IP : 10.104.52.241, Dest Port : 9991, Src Port : 0, State : UP
 Source Interface : Loopback0, MD5 Disabled
 Hello Timer 0 sec, Dead Timer 0 sec, Next Hello 00:00:00
 Uptime 00:00:00
Service Announcement :
 Filter : policy1
 Count 100, Delay Timer 30 sec, Pending Announcement 0, Pending Withdraw
 0
 Total Export Count 300, Next Export in 00:00:16
Service Query :
 Query Suppression Disabled
 Query Count 50, Query Delay Timer 15 sec, Pending 0
 Total Query Count 0, Next Query in 00:00:01
```

Verifying mDNS Cache Configurations

The following show commands display cache from both Active and Standby devices using the chassis option:

```
Device# show mdns-sd cache chassis active R0

------------------------------------------------------------ PTR Records
------------------------------------------------------------------
```

```
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------------------
_home-sharing._tcp.local                       4500     WLAN      1     0205.2c23.0001
AP6B8B4567-sta00001._home-sharing._tcp.local

------------------------------------------------------------------ SRV Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------------------
AP6B8B4567-sta00001._home-sharing._tcp.local   4500     WLAN      1     0205.2c23.0001   0
 0 5353 AP6B8B4567-sta00001.local

------------------------------------------------------------- A/AAAA Records
------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------------------
AP6B8B4567-sta00001.local                      4500     WLAN      1     0205.2c23.0001
9.2.57.106

------------------------------------------------------------------ TXT Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------------------
AP6B8B4567-sta00001._home-sharing._tcp.local   4500     WLAN      1     0205.2c23.0001
[14]'model=MacMini'
```

Note Alternatively, you can issue the **show mdns-sd cache** command to display the cache from the Active controller.

```
Device# show mdns-sd cache chassis standby R0

------------------------------------------------------------------ PTR Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------------------
_home-sharing._tcp.local                       4500     WLAN      1     0205.2c23.0001
AP6B8B4567-sta00001._home-sharing._tcp.local

------------------------------------------------------------------ SRV Records
------------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------------------
AP6B8B4567-sta00001._home-sharing._tcp.local   4500     WLAN      1     0205.2c23.0001   0
 0 5353 AP6B8B4567-sta00001.local

------------------------------------------------------------- A/AAAA Records
------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
------------------------------------------------------------------------------------------------------------------------
AP6B8B4567-sta00001.local                      4500     WLAN      1     0205.2c23.0001
9.2.57.106

------------------------------------------------------------------ TXT Records
```

```
-------------------------------------------------------------
RECORD-NAME                                    TTL      TYPE      ID    CLIENT-MAC
RR-RECORD-DATA
-------------------------------------------------------------------------------------------------
AP6B8B4567-sta00001._home-sharing._tcp.local   4500     WLAN      1     0205.2c23.0001
[14]'model=MacMini'
```

Verifying Additional mDNS Cache Configurations

To verify the cache from the Active DB, use the following commands:

```
show mdns-sd cache ap-mac 0a0b.0cf0.000e chassis active R0
show mdns-sd cache client-mac 0269.fe06.0023 chassis active R0
show mdns-sd cache detail chassis active R0
show mdns-sd cache glan-id <> chassis active R0
show mdns-sd cache glan-id <> detail chassis active R0
show mdns-sd cache location-group <> chassis active R0
show mdns-sd cache location-group <> detail chassis active R0
show mdns-sd cache mdns-ap <> detail chassis active R0
show mdns-sd cache mdns-ap <> chassis active R0
show mdns-sd cache rlan-id <> detail chassis active R0
show mdns-sd cache rlan-id <> chassis active R0
show mdns-sd cache type TXT chassis active R0
show mdns-sd cache type A-AAAA detail chassis active R0
show mdns-sd cache wired chassis active R0
show mdns-sd cache wired detail chassis active R0
show mdns-sd cache wlan-id 10 chassis active R0
show mdns-sd cache wlan-id 1 detail chassis active R0
```

To verify the cache from the Standby DB, use the following commands:

```
show mdns-sd cache ap-mac <> chassis standby R0
show mdns-sd cache client-mac <> chassis standby R0
show mdns-sd cache detail chassis standby R0
show mdns-sd cache glan-id <> chassis standby R0
show mdns-sd cache glan-id <> detail chassis standby R0
show mdns-sd cache location-group <> chassis standby R0
show mdns-sd cache location-group <> detail chassis standby R0
show mdns-sd cache mdns-ap <> detail chassis standby R0
show mdns-sd cache mdns-ap <> chassis standby R0
show mdns-sd cache rlan-id <> detail chassis standby R0
show mdns-sd cache rlan-id <> chassis standby R0
show mdns-sd cache type [A-AAAA|PTR|SRV|TXT] chassis standby R0
show mdns-sd cache type [A-AAAA|PTR|SRV|TXT] detail chassis standby R0
show mdns-sd cache wired chassis standby R0
show mdns-sd cache wired detail chassis standby R0
show mdns-sd cache wlan-id <> chassis standby R0
show mdns-sd cache wlan-id <> detail chassis standby R0
```

Verifying Local Area Bonjour Configuration for LAN and Wireless Networks

The following is a sample output of the **show run** command.

```
mdns-sd gateway

mdns-sd service-definition custom1
```

```
 service-type _airplay._tcp.local
 service-type _raop._tcp.local


mdns-sd service-list list1 IN
 match custom1
mdns-sd service-list list2 OUT
 match custom1


mdns-sd service-policy policy1
service-list list1 IN
service-list list2 OUT


service-export mdns-sd controller Cisco Catalyst Center-CONTROLLER-POLICY
controller-address 99.99.99.10
controller-service-policy policy1 OUT
controller-source-interface Loopback0
```

Additional References for DNA Service for Bonjour

Related Topic	Document Title
Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide	Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide, Release 1.3.1.0

MIBs

MIB	MIBs Link
CISCO-SDG-MDNS-MIB	This MIB module defines objects describing the statistics of 63 local area and wide area mDNS SDG agent. Statistics could be 64 either global or per interface specific.

Feature History for Cisco DNA Service for Bonjour

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Release	Modification
Cisco IOS 15.2(6) E2	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour was introduced on the following platforms: • Cisco Catalyst 2960-X Series Switches • Cisco Catalyst 2960-XR Series Switches
Cisco IOS 15.5(1)SY4	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour was introduced on Cisco Catalyst 6800 Series Switches.
Cisco IOS XE 3.11.0 E	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour was introduced on the following platforms: • Cisco Catalyst 4500-E Series Switches • Cisco Catalyst 4500-X Series Switches
Cisco IOS XE Gibraltar 16.11.1	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour was introduced on the following platforms: • Cisco Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 9300 Series Switches • Cisco Catalyst 9400 Series Switches • Cisco Catalyst 9500 Series Switches • Cisco Catalyst 9500 Series Switches - High Performance • Cisco Catalyst 9600 Series Switches • Cisco Catalyst 9800 Series Wireless Controllers • Cisco 5500 Series Wireless Controllers • Cisco 8540 Wireless Controllers • Cisco 4000 Series Integrated Services Routers (ISR)
Cisco IOS XE Amsterdam 17.1.1	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour was introduced on Cisco Catalyst 9200 Series Switches.

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	Introduced Cisco DNA Service for Bonjour support for the following: • SD-Access network • Unicast mode for LAN network
Cisco IOS XE Amsterdam 17.3.2a	Introduced Cisco DNA Service for Bonjour support for the following: • Multilayer networks • Location grouping in wired networks • mDNS AP group in wireless networks
Cisco IOS XE Bengaluru 17.6.1	Introduced support for the following features for Local Area Bonjour in Unicast Mode for LAN networks: • Default mDNS Service Configurations • HSRP-Aware mDNS Service-Routing • mDNS Service-Gateway SSO Support

CHAPTER 193

Configuring Local Area Bonjour for Wireless Local Mode

- Overview of Local Area Bonjour for Wireless Local Mode, on page 2201
- Prerequisites for Local Area Bonjour for Wireless Local Mode, on page 2201
- Restrictions for Local Area Bonjour for Wireless Local Mode, on page 2202
- Understanding Local Area Bonjour for Wireless Local Mode, on page 2202
- Configuring Wireless AP Multicast, on page 2203
- Configuring Local Area Bonjour for Wireless Local Mode, on page 2206
- Verifying mDNS Gateway Configuration, on page 2217
- Reference, on page 2219

Overview of Local Area Bonjour for Wireless Local Mode

The Cisco Catalyst 9800 series controller introduces unicast mode function in Local Area Bonjour network domain. The enhanced gateway function at the first hop of Wired and Wireless networks communicates directly with any industry standard RFC 6762 compliant Multicast DNS (mDNS) end point in Layer 2 Unicast mode. The controller also introduces new service-peer mode expanding classic single-gateway controller to end-to-end service-routing with upstream SDG agent switch to enable unicast-mode, increased scale, performance and resiliency in the network.

Prerequisites for Local Area Bonjour for Wireless Local Mode

The Cisco Catalyst 9800 series controller must be successfully configured and be operational before implementing Cisco Local Area Bonjour for local mode wireless networks.

The following list provides the prerequisites for the controller that is to be deployed in service-peer mode:

- Ensure that the targeted controller for the service-peer role has the required Cisco IOS-XE software version. See *Supported SDG Agents with Supported Licenses and Software Requirements* table in Cisco DNA Service for Bonjour Solution Overview chapter.
- Ensure that the controller runs a valid Cisco DNA-Advantage license.
- Ensure that the upstream distribution-layer Cisco Catalyst switch in SDG agent mode runs a valid Cisco DNA-Advantage license.

- Ensure that the controller is interconnected as Layer 2 trunk in static 802.1Q mode, when Layer 2 Unicast service-routing is running between SDG agent in distribution-layer and the controller service-peer.
- Ensure that the controller has IP reachability to upstream Cisco Catalyst 9000 series switches in SDG agent mode over same the IPv4 wireless management subnet.
- Ensure that global multicast is enabled on the controller and AP is set to multicast mode. All local mode APs must join the multicast group in the network to successfully process mDNS messages.

Restrictions for Local Area Bonjour for Wireless Local Mode

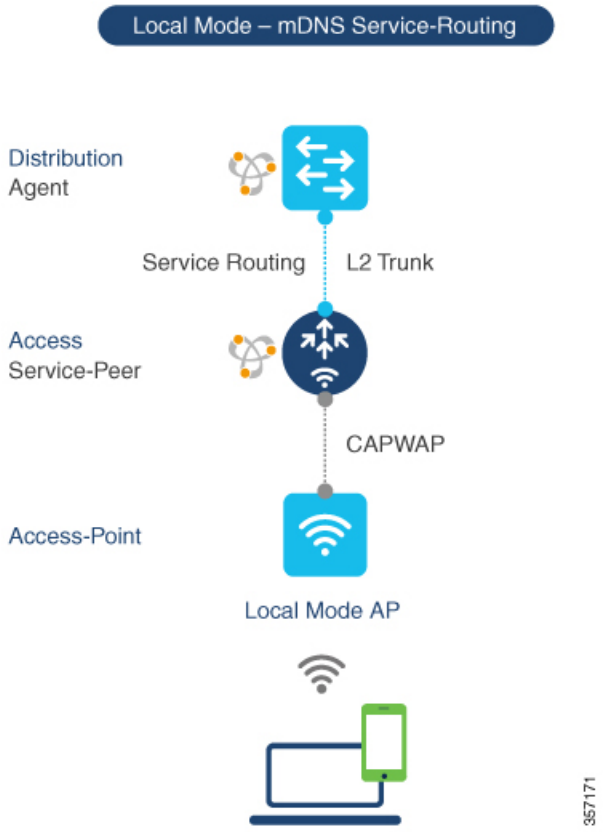
- Controller management port is not supported for service-routing with upstream Catalyst SDG Agent switch.
- The controller in service peer mode supports location-based service for access points in local mode and FlexConnect central switching mode.
- The controller supports location-based capabilities only between wireless connected service provider and the receiver.
- The controller does not support service-routing configuration using GUI.

Understanding Local Area Bonjour for Wireless Local Mode

The traditional wireless controller supported mDNS snooping function with various advancements for wireless networks. As the enterprise requirements expands, it drives the IT organization to introduce new network deployment models, supporting mobile devices and distributed zero-configuration services following increased scale, granular security control and resiliency for mission critical networks. The unified Cisco IOS-XE operating system across Cisco Catalyst 9000 series LAN switches and Cisco Catalyst 9800 series controller enables distributed Bonjour gateway function at the network edge. With end-to-end Wide Area Bonjour service-routing, the new solution enables service-oriented enterprise networks with intuitive user-experience.

The following figure illustrates the controller platform supporting mDNS gateway function to wireless users in local mode and builds service-routing peering with upstream Cisco Catalyst 9000 series switch for network-wide services discovery and distribution based on IT-managed granular policies and locations. The unicast based service-routing between the controller in service-peer mode and upstream SDG-Agent switch eliminates mDNS flooding over Layer 2 trunk ports and provide increase bandwidth and eliminates mDNS flood over wireless networks and Layer 2 trunk to upstream network.

Figure 71: Cisco Catalyst 9800 Series Controller Local Area Bonjour for Wireless Local Mode

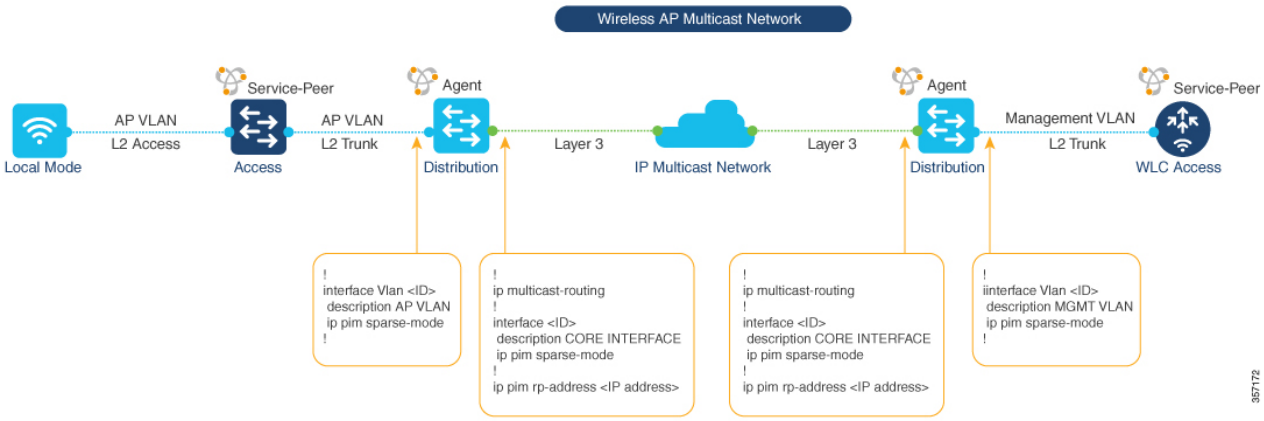


Configuring Wireless AP Multicast

The controller and AP by default prevents forwarding of Layer 2 or Layer 3 Multicast frames between wireless and wired network infrastructure. The forwarding is supported with stateful capabilities enabled using AP multicast. To allow mDNS message processing over a wireless network, multicast must be enabled and unique AP multicast group must be configured on the controller to advertise in IP core network. This AP multicast group is only required for APs to enable Multicast over Multicast (MCMC) capabilities in the network. The Bonjour solution do not require any other multicast requirements on wireless client VLAN; thus, it is optional and applicable only for other Layer 3 multicast applications.

The figure given below illustrates end-to-end wireless multicast configuration requirement to ensure wireless APs successfully join the controller-announced multicast group.

Figure 72: Multicast Routing in IP Core Network



Configuring Wireless AP Multicast (GUI)

This procedure configures wireless AP multicast on a controller in service-peer mode.

Procedure

Step 1 Choose **Configuration** > **Services** > **Multicast**.

Step 2 Set the **Global Wireless Multicast Mode** to **Enabled**.

Step 3 From the AP Capwap Multicast drop-down list, select **Multicast**.

Step 4 Enter a unique IP address at **AP Capwap IPv4 Multicast group Address**.

Step 5 Click **Apply**.

Step 6 Click **Save**.

Configuring Wireless AP Multicast (CLI)

This procedure configures wireless AP multicast on a controller in service-peer mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless multicast** **Example:** `Device(config)# wireless multicast`	Enable global IP multicast processing.

	Command or Action	Purpose
Step 3	**wireless multicast** *IPv4-multicast-address* **Example:** `Device(config)# wireless multicast 239.254.254.1`	Enables AP CAPWAP mode to Multicast with unique IPv4 multicast address configurations.
Step 4	**exit** **Example:** `Device(config-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

Configuring Multicast in IP Network (CLI)

This procedure configures IP Multicast under AP VLAN, Management VLAN and IP core interfaces on upstream Catalyst LAN distribution-layer switch.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip multicast-routing** **Example:** `Device(config)# ip multicast-routing`	Enables IP multicast processing.
Step 3	**interface** *interface-id* **Example:** `Device(config)# interface TenGigabitEthernet 1/0`	Selects an interface that is connected to hosts and network devices on which PIM can be enabled.
Step 4	**ip pim sparse-mode** **Example:** `Device(config-if)# ip pim sparse-mode`	Enables IP Multicast on Layer 3 interfaces of distribution and core layer network switches: • **AP VLAN**– Enables IP multicast on SVI interface on VLAN assigned to wireless APs of wireless AP distribution layer switch. • **Management VLAN**– Enables IP multicast on SVI interface on VLAN assigned to controller management VLAN of wireless distribution layer switch. • **Layer 3 Interface**– Enable IP multicast routing on all core network devices and Layer 3 interfaces.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 6	**ip pim rp-address** *rp-address* **Example:** `Device(config)# ip pim rp-address 239.254.254.100`	Configures IP Multicast RP address on core and distribution network switches. IP network may have alternate multicast routing method.

Configuring Local Area Bonjour for Wireless Local Mode

This section provides configuration guidelines to implement Cisco Catalyst 9800 series controller as mDNS gateway and enable service-peer mode to enable service-routing with upstream distribution-layer Cisco Catalyst 9000 series switch in SDG-Agent mode to build Local Area Bonjour.

Configuring mDNS Service Policy (GUI)

The mDNS service policy consists of creating a service-list to permit built-in or user-defined custom service-types, associate service-list to a service-policy to enforce in ingress or egress direction and apply the service-policy to targeted Wireless Profile. This configuration is common on the controller in service peer or single-gateway solution for wireless networks.

This procedure configures mDNS Service-Policy on a controller in service-peer mode.

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS**.

Step 2 Set the mDNS Gateway button to **Enabled**.

Step 3 Click **Service Policy** Tab.

Step 4 Click **Service List** and click **Add**.

This activates the Service List window.

Step 5 In the **Service List Name** field, enter a unique name with alphanumeric value.

Step 6 From the **Direction** drop-down list, select service list policy direction. Use **IN** for ingress or **OUT** for egress mDNS message matching policy.

Step 7 Click **+Add Services** to add mDNS service-types in selected service list.

Step 8 From the **Available Services** drop-down list, select built-in or custom mDNS service-type.

Step 9 From the **Message Type** drop-down list, select **Announcement** to accept service advertisement or **Query** to permit service discovery from the network. Default message-type is **any**.

Step 10 Click **Save** button to add mDNS service-type entry.

Note Repeat Step-7 to Step-9 to add more mDNS service-types in selected service list.

Step 11 Click **Apply to Device**.

This creates a new mDNS Service List for selected direction.

Note Repeat Step-5 to Step-11 for bi-directional service list.

Step 12 Click **Service-Policy** tab.

Step 13 Click **+Add** to create new mDNS service-policy.

Step 14 In the **Service Policy Name** field, enter a unique mDNS service policy name.

Step 15 From the **Service List Input** drop-down list, select ingress mDNS service list input to enforce mDNS policies on ingress direction from wireless networks.

Step 16 From the **Service List Output** drop-down list, select mDNS policies on egress direction to wireless networks.

Step 17 Click **Apply to Device**.

This creates a new mDNS service policy.

Step 18 Choose **Configuration** > **Tags & Profiles** > **Policy**

Step 19 Choose or create a new **Policy Profile**.

Step 20 Click **Advanced** tab.

Step 21 From the **mDNS Service Policy** drop-down list, select an mDNS service policy.

Refer to Cisco Catalyst 9800 Series Configuration Guide to configure other policy profile parameters.

Step 22 Click **Apply to Device** button.

This creates a new policy profile or updates an existing policy profile with mDNS service policy.

Step 23 Click **Save**.

Configuring mDNS Service Policy (CLI)

This procedure builds and applies service-policies on target wireless profile in service-peer mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 2	**mdns-sd service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config)# mdns-sd service-list VLAN100-LIST-IN in`
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
		Configures mDNS service-list to classify one or more service-types. Unique service-list is required to process incoming mDNS message and outbound response to requesting end points.

	Command or Action	Purpose

Step 3	**match service-definition-name** [**message-type** {**any** | **announcement** | **query**}]
	Example:
	`Device(config)# mdns-sd service-list VLAN100-LIST-IN in`
	`Device(config-mdns-sl-in)# match APPLE-TV`
	`Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`
		Matches inbound service-list. The controller validates to accept or drop incoming mDNS service-type (for example, Apple TV) advertisement or query matching message type. The service-list contains implicit deny at the end. Default message-type is "any".

Step 4	**match service-definition-name** [**message-type** {**any** | **announcement** | **query**}]
	Example:
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
	`Device(config-mdns-sl-in)# match APPLE-TV`
	`Device(config-mdns-sl-in)# match PRINTER-IPPS`
		Matches an outbound service-list. The controller provides local service proxy function by responding matching service-type to the requesting end points. For example, the Apple-TV and Printer learnt from VLAN 100 will be distributed to receiver in same VLAN 100. The service-list contains implicit deny at the end.
		The message-type for outbound service-list is not required.

Step 5	**exit** **Example:** `Device(config-mdns-sl-in)# exit`	Returns to global configuration mode.
Step 6	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy VLAN100-POLICY`	Creates a unique mDNS service-policy.

Step 7	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-IN in`
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-OUT out`
		Configure mDNS service-policy to associate service-list for each direction.

Step 8	**exit** **Example:** `Device(config-mdns-ser-policy)# exit`	Exits mDNS service policy configuration mode.
Step 9	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy WLAN-PROFILE`	Configures unique wireless profile policy name to associate mDNS service-policy.

	Command or Action	Purpose
Step 10	**mdns-sd service-policy** *service-policy* **Example:** `Device(config-wireless-policy)# mdns-sd service-policy VLAN100-POLICY`	Associates mDNS service-policy to configured VLAN IDs. **Note** This step requires wireless profile policy to be administratively shutdown prior association service-policy and re-activate with no shutdown to make service-policy effective.
Step 11	**exit** **Example:** `Device(config-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

Configuring Custom Service Definition (GUI)

The Cisco IOS-XE supports various built-in well-known mDNS service-definition types mapping to key mDNS PTR records to user-friendly names. For example, built-in Apple-TV service-type is associated with _airplay. _tcp.local and _raop. _tcp.local PTR records to successfully enable service in the network. The network administrator can create custom service-definition with matching mDNS PTR records to enable end mDNS service-routing in the network.

This procedure configures custom mDNS service definition and applies it to policy.

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS**.

Step 2 Set the mDNS Gateway button to **Enabled**.

Step 3 Click **Service Policy** Tab.

Step 4 Click **Add** to create new custom mDNS service-list definition.

This activates Service Definition window.

Step 5 In the **Service Definition Name** filed, enter a unique aplhanumeric value.

Step 6 (Optional) In the **Description** field, enter a description for the service definition.

Step 7 In the **Service Type** field, enter single mDNS PoinTeR (PTR) record entry in ***_<service-type>._<protocol>.local*** regular expression format. For example, _airplay. _tcp.local

Step 8 Click **+** to add custom mDNS service-type in selected definition list.

Note Repeat Steps 7 and Step 8 to add more custom service-type in selected definition list.

Step 9 Click **Apply**.

Step 10 Perform steps give in *Configuring mDNS Service Policy (GUI)* by selecting built-in or custom service-type to configure service list.

Step 11 Click **Save**.

Configuring Custom Service Definition (CLI)

This procedure creates custom service-definition configuration to discover mDNS services from local wireless networks.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd service-definition-name** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition APPLE-CLASSROOM`	Creates unique service-definition name for custom service-types.
Step 3	**service-type** *custom-mDNS-PTR* **Example:** `Device(config-mdns-ser-def)# service-type _classroom._tcp.local`	Configure an regular-expression string for custom mDNS PoinTeR(PTR) record.
Step 4	**exit** **Example:** `Device(config-mdns-ser-def)# exit`	Returns to global configuration mode.

Configuring mDNS Gateway on WLAN (GUI)

The mDNS gateway activation on targeted WLAN is required to start processing incoming mDNS messages from associated wireless clients. To activate mDNS gateway the WLAN must be administratively shutdown and re-enable thus it may require network downtime planning.

This procedure configures custom mDNS gateway and required policies.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click to enable the mDNS Gateway on existing **WLAN** row of Catalyst 9800 controller. Click **+ Add** button to create new WLAN if required. Refer to Catalyst 9800 Series Wireless Controller Configuration Guide for step-by-step WLAN configuration.

Step 3 Click **Advanced** tab.

Step 4 From the **mDNS Mode** drop-down list, select **Gateway** to activate mDNS Gateway on the selected WLAN.

Step 5 Click **Apply to Device**.

Step 6 Click **Save**.

Configuring mDNS Gateway on WLAN (CLI)

This procedure implements mDNS gateway on a targeted WLAN of the controller in service-peer mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name WLAN-ID SSID-name* **Example:** `Device(config)# wlan WLAN-PROFILE 1 blizzard`	Creates a unique WLAN.
Step 3	**mdns-sd-interface gateway** **Example:** `Device(config-wlan)# mdns-sd-interface gateway`	Configure mDNS gateway on targeted WLAN. **Note** This step requires wireless profile policy to be administratively shutdown prior association service-policy and re-activate with no shutdown to make service-policy effective.
Step 4	**exit** **Example:** `Device(config-wlan)# exit`	Returns to global configuration mode.

Configuring Service-Routing on Service-Peer

The controller deployed in Service-Peer mode extends mDNS service discovery and distribution boundary beyond single controller to global IP network using on unicast based service-routing. The controller service peer must establish IP based unicast service-routing with Cisco Catalyst 9000 series switch in distribution layer network for global service-routing.

This procedure configures the controller in service peer mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS and enters in mDNS gateway configuration mode. The following optional parameters are available: • **active-query**: Periodic mDNS query to refresh dynamic cache. • **active-response**: Periodic active mDNS response instead per request processing. • **mode**: Set Catalyst 9800 in service-peer mode. • **sdg-agent**: Unicast service-routing with targeted SDG-Agent. • **service-announcement-count**: Configures maximum advertisements in service-routing to SDG-Agent. • **service-announcement-timer**: Configures advertisements announce timer periodicity in service-routing to SDG-Agent. • **service-query-count**: Configures maximum queries in service-routing to SDG-Agent. • **service-query-timer**: Configures query forward timer periodicity in service-routing to SDG-Agent. • **service-type-enumeration**: Configures service enumeration. • **source-interface**: Configures the source interface. If the source interface is configured, it will be used for all mDNS transactions. By default, wireless management interface will be used. • **transport**: Use IPv4 (default) or IPv6 transport for mDNS messaging to end points.

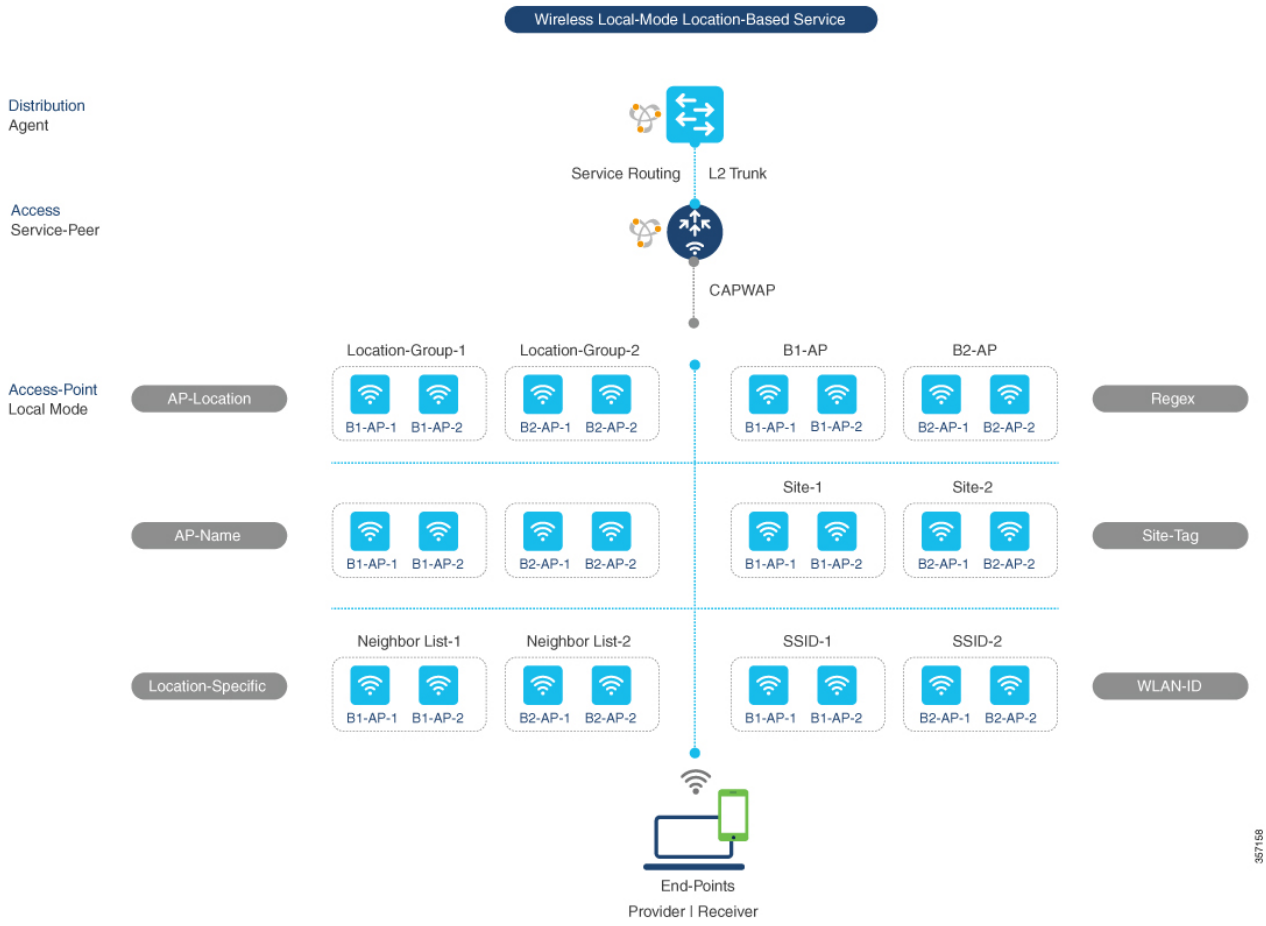
	Command or Action	Purpose
		Note For **rate-limit**, **service-announcement-count**, **service-announcement-timer**, **service-query-count** and **service-query-timer** commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.
Step 3	**mode** [**service-peer**] **Example:** `Device(config-mdns-sd)# mode service-peer`	Configure mDNS gateway in service-peer mode.
Step 4	**sdg-agent** [**IPv4 Address**] **Example:** `Device(config-mdns-sd)# sdg-agent 10.0.2.254`	Configure SDG Agent IPv4 address. Typically, the management VLAN gateway address. If FHRP mode, then use FHRP Virtual-IP address of management VLAN.
Step 5	**exit** **Example:** `Device(config-mdns-sd)# exit`	Returns to global configuration mode.

Configuring Location-Based mDNS on Service-Peer (GUI)

Cisco Catalyst 9800 series controller supports location-based mDNS service discovery and distribution between wireless service provider and receiver endpoints. The location-based mDNS service support can be implemented using multiple supporting AP classification methods to implement policy-based service distributions in wireless networks. The location-based mDNS service is effective and supported on wireless APs in Local-Mode or FlexConnect Central Switching modes.

The figure given below illustrates various LSS based mDNS service mode discovery and distribution support:

Figure 73: Location-Based mDNS Gateway



This procedure configures location-based mDNS service policy.

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS**.

Step 2 Set the mDNS Gateway button to **Enabled**.

Step 3 Click **Service Policy** Tab.

Step 4 Click **Service List** and click **Add**.

This activates the Service List window.

Step 5 In the **Service List Name** field, enter a unique name with alphanumeric value.

Step 6 From the **Direction** drop-down list, select service list policy direction. Use **IN** for ingress or **OUT** for egress mDNS message matching policy.

Step 7 Click **+Add Services** to add mDNS service-types in selected service list.

Step 8 From the **Available Services** drop-down list, select built-in or custom mDNS service-type.

Step 9 From the **Message Type** drop-down list, select **Announcement** to accept service advertisement or **Query** to permit service discovery from the network. Default message-type is **any**.

Step 10 Click **Save** button to add mDNS service-type entry.

Note Repeat Step-7 to Step-9 to add more mDNS service-types in selected service list.

Step 11 Click **Apply to Device**.

This creates a new mDNS Service List for selected direction.

Note Repeat Step-5 to Step-11 for bi-directional service list.

Step 12 Click **Service-Policy** tab.

Step 13 Click **+Add** to create new mDNS service-policy.

Step 14 In the **Service Policy Name** field, enter a unique mDNS service policy name.

Step 15 From the **Service List Input** drop-down list, select ingress mDNS service list input to enforce mDNS policies on ingress direction from wireless networks.

Step 16 From the **Service List Output** drop-down list, select mDNS policies on egress direction to wireless networks.

Step 17 Click **Apply to Device**.

This creates a new mDNS service policy.

Step 18 Choose **Configuration** > **Tags & Profiles** > **Policy**

Step 19 Choose or create a new **Policy Profile**.

Step 20 Click **Advanced** tab.

Step 21 From the **mDNS Service Policy** drop-down list, select an mDNS service policy.

Refer to Cisco Catalyst 9800 Series Configuration Guide to configure other policy profile parameters.

Step 22 Click **Apply to Device** button.

This creates a new policy profile or updates an existing policy profile with mDNS service policy.

Step 23 Click **Save**.

Configuring Location-Based mDNS on Service-Peer (CLI)

This procedure implements LSS based mDNS service discovery and distribution between wireless endpoints on the targeted WLAN of the controller in service-peer mode.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy VLAN100-POLICY`	Creates a unique mDNS service-policy.
Step 3	**location** {**ap-location** | **ap-name** | **lss** | **regex** | **site-tag** | **ssid**} **Example:** `Device(config-mdns-ser-policy)# location ap-location`	Creates a unique mDNS service-policy. • **ap-location**: Enables mDNS service discovery and distribution between wireless service provider and receiver connected to one or more AP configured in the same location name. The mDNS services from non-matching AP location is automatically filtered. • **ap-name**: Enables mDNS service discovery and distribution between wireless service provider and receiver connected to single AP matching same AP name. The mDNS services from non-matching AP name is automatically filtered. • **lss**: Enables mDNS service discovery and distribution between wireless service provider and receiver connected to same and neighboring one or more AP based on RRM. The mDNS services from non-matching AP neighbor-list is automatically filtered. • **regex**: Enables mDNS service discovery and distribution between wireless service provider and receiver connected to one or more AP configured within matching AP name or AP Location name using regular-expression string. The mDNS services from non-matching AP names is automatically filtered. • **site-tag**: Enables mDNS service discovery and distribution between wireless service provider and receiver connected to one or more AP configured same site tag name. The mDNS services from non-matching site tag is automatically filtered. • **ssid**: Enables mDNS service discovery and distribution between wireless service provider and receiver connected to one or more AP configured same SSID name. The

	Command or Action	Purpose
		mDNS services from non-matching SSID is automatically filtered.
Step 4	**exit** **Example:** `Device(config-mdns-ser-policy)# exit`	Exits mDNS service policy configuration mode.

Verifying mDNS Gateway Configuration

This section provides guidelines to verify various Local Area Bonjour domain mDNS service configuration parameters, cache records, statistics and more on the controller in service peer mode.

Table 148:

Command or Action	Purpose
show mdns-sd cache { **ap-mac** | **client-mac** | **detail** | **glan-ID** | **mdns-ap** | **rlan-id** | **statistics** | **type** | **udn** | **wired** | **wlan-id** }	Displays available mDNS cache records supporting multiple following variables providing granular source details: • **ap-mac**: Displays one or more mDNS service instance cache records discovered from provided AP MAC address. • **client-mac**: Displays one or more mDNS service instance(s) cache records discovered from service provider wireless client MAC address. • **detail**: Displays mDNS record detail information combined with client and network attributes and other service parameters. • **glan-ID**: Displays one or more mDNS service instance(s) cache records discovered from provided Wired Guest LAN ID MAC address. • **mdns-ap**: Displays one or more mDNS service instance(s) cache records discovered from provided Wireless mDNS AP MAC address. • **rlan-id**: Displays one or more mDNS service instances(s) cache records discovered from provided Wired Remote LAN ID. Range 1-128. • **statistics**: Displays detail global bi-directional mDNS statistics for IPv4 and IPv6 transports with packet processing count for each mDNS record-type. • **type**: Displays one or more service-instance(s) cache records matching mDNS record-type, i.e., A-AAAA, PTR, SRV and TXT. • **udn**: Displays one or more mDNS service instance(s) cache records discovered from segmented Wireless service provider in User-Defined-Group (UDN) or shared-services. • **wired**: Displays one or more mDNS service instance(s) cache records discovered from upstream Layer 2 wired network. • **wlan-id**: Displays one or more mDNS service instance(s) cache records discovered from matching provided wlan-ID. Range 1-4096.

Command or Action	Purpose
show mdns-sd statistics {**debug** | **flexconnect** | **glan-id** | **rlan-id** | **wired** | **wlan-id**}	Displays detailed mdns statistics processed bi-directionally by system on each mDNS gateway enabled VLAN configured mDNS in Unicast mode. The expanded keyword of mDNS statistics can provide detail view on interface, policy, service-list and services.
show mdns-sd summary	Displays brief information about mDNS gateway and key configuration status on all VLANs and interfaces of the system.

Verifying Catalyst WLC Service-Peer Configuration

This section provides guidelines to verify service peer service configuration and statistics.

Table 149:

Command or Action	Purpose
show mdns-sd sp-sdg statistics	Displays mDNS service-routing statistics between Catalyst 9800 service-peer and upstream SDG Agent switch for global service discovery and distribution.
show mdns-sd summary	Displays brief information about mDNS gateway and key configuration status and parameters of the system.

Reference

Table 150:

Related Topic	Document Title
DNA Service for Bonjour Deployment on Cisco Catalyst 9600 Switch	Cisco Catalyst 9600 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9500 Switch	Cisco Catalyst 9500 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9400 Switch	Cisco Catalyst 9400 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9300 Switch	Cisco Catalyst 9300 Series Switch Software Configuration Guide, Release 17.5.X
Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide	Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide, Release 2.2.2

CHAPTER 194

Configuring Local Area Bonjour for Wireless FlexConnect Mode

- Overview of Local Area Bonjour for Wireless FlexConnect Mode, on page 2221
- Restrictions for Local Area Bonjour for Wireless FlexConnect Mode, on page 2221
- Prerequisites for Local Area Bonjour for Wireless FlexConnect Mode, on page 2222
- Understanding mDNS Gateway Alternatives for Wireless FlexConnect Mode, on page 2222
- Understanding Local Area Bonjour for Wireless FlexConnect Mode, on page 2224
- Configuring Local Area Bonjour for Wireless FlexConnect Mode, on page 2226
- Verifying Local Area Bonjour in Service-Peer Mode, on page 2239
- Verifying Local Area Bonjour in SDG Agent Mode, on page 2241
- Reference, on page 2243

Overview of Local Area Bonjour for Wireless FlexConnect Mode

The Cisco Catalyst 9800 series controller introduces unicast mode function in Local Area Bonjour network domain. The enhanced gateway function at the first hop of Wired and Wireless networks communicates directly with any industry standard RFC 6762 compliant Multicast DNS (mDNS) end point in Layer 2 Unicast mode. The controller also introduces new service-peer mode expanding single-gateway to end-to-end service-routing with upstream SDG-Agent switch to enable unicast-mode, increased scale, performance and resiliency in the network.

Restrictions for Local Area Bonjour for Wireless FlexConnect Mode

- In FlexConnect mode network deployments, the mDNS gateway and service-peer mode on the controller must not be configured and must be in disabled state.

Prerequisites for Local Area Bonjour for Wireless FlexConnect Mode

The Cisco Catalyst 9800 series controller must be successfully configured and operational before implementing Cisco Local Area Bonjour for FlexConnect mode wireless networks.

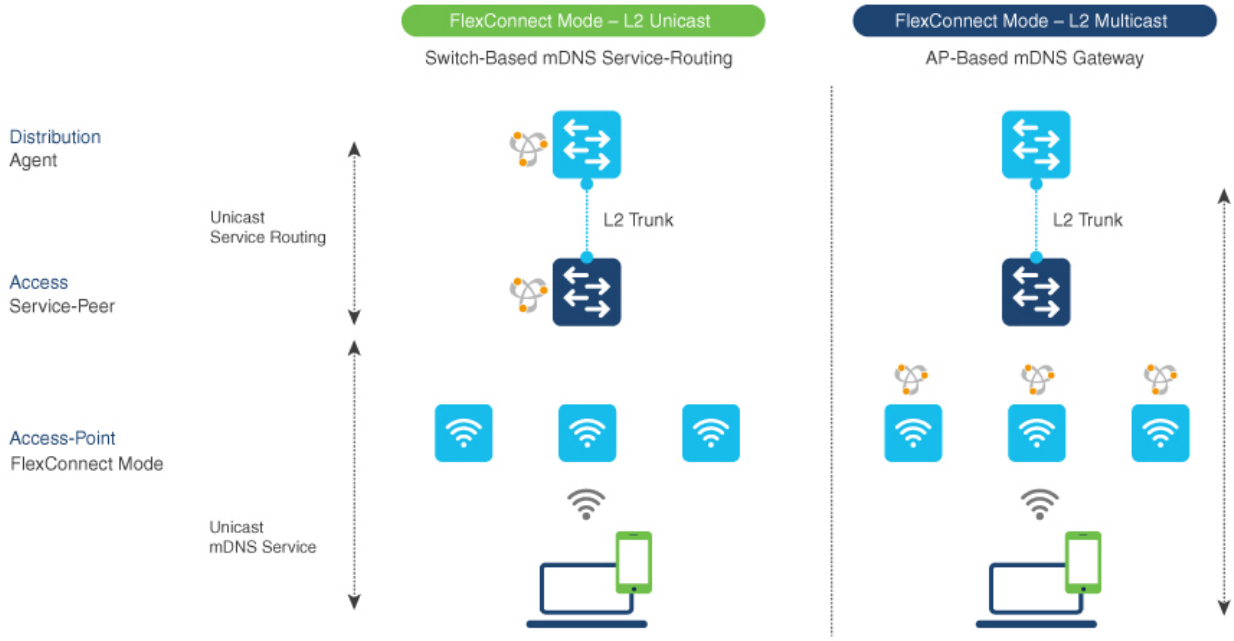
The following list provides the prerequisites for the controller that is to be deployed to enable successful mDNS gateway solution for Wireless FlexConnect:

- Ensure that the targeted Layer 2 Catalyst 9000 Series Ethernet switch is configured in service-peer role and running the required Cisco IOS-XE software version.
- Ensure that the Catalyst 9000 Series Ethernet switch runs a valid Cisco DNA-Advantage license.
- Ensure that the upstream distribution-layer Cisco Catalyst switch for Wired and FlexConnect Local Switching Wireless networks is configured in SDG-Agent mode and runs a valid Cisco DNA-Advantage license.

Understanding mDNS Gateway Alternatives for Wireless FlexConnect Mode

The controller continues to innovate mDNS gateway function to address evolving business and technical requirements in the Enterprise networks. The FlexConnect Local Switching based wireless networks implement mDNS gateway using the following two methods depicted in the figure:

Figure 74: mDNS Gateway Alternatives for FlexConnect Mode



Based on the operating network environment, the mDNS gateway for FlexConnect mode wireless network can be implemented in one of the following modes to address service discovery and distribution:

- **Switch Based mDNS Gateway**—In Layer 2 access, the Cisco Catalyst 9000 series Ethernet switch must be implemented as mDNS gateway in Service-Peer role. The following are the key benefits:
  - Replaces flood-n-learn with the new enhanced Unicast-based mDNS communication with FlexConnect mode wireless users.
  - Eliminates mDNS flood with Unicast service-routing to LAN distribution. The Unicast service-routing between LAN distribution and Layer 2 access layer switches forms Local Area Bonjour domain to enable policy and location-based service discovery and distribution. The Unicast based service-routing over Layer 2 trunk eliminates mDNS flood-free and enables service-oriented wireless networks.
  - Eliminates the requirement to forward wired network traffic to wireless Access Points improving wireless scale, performance, and network reliability.

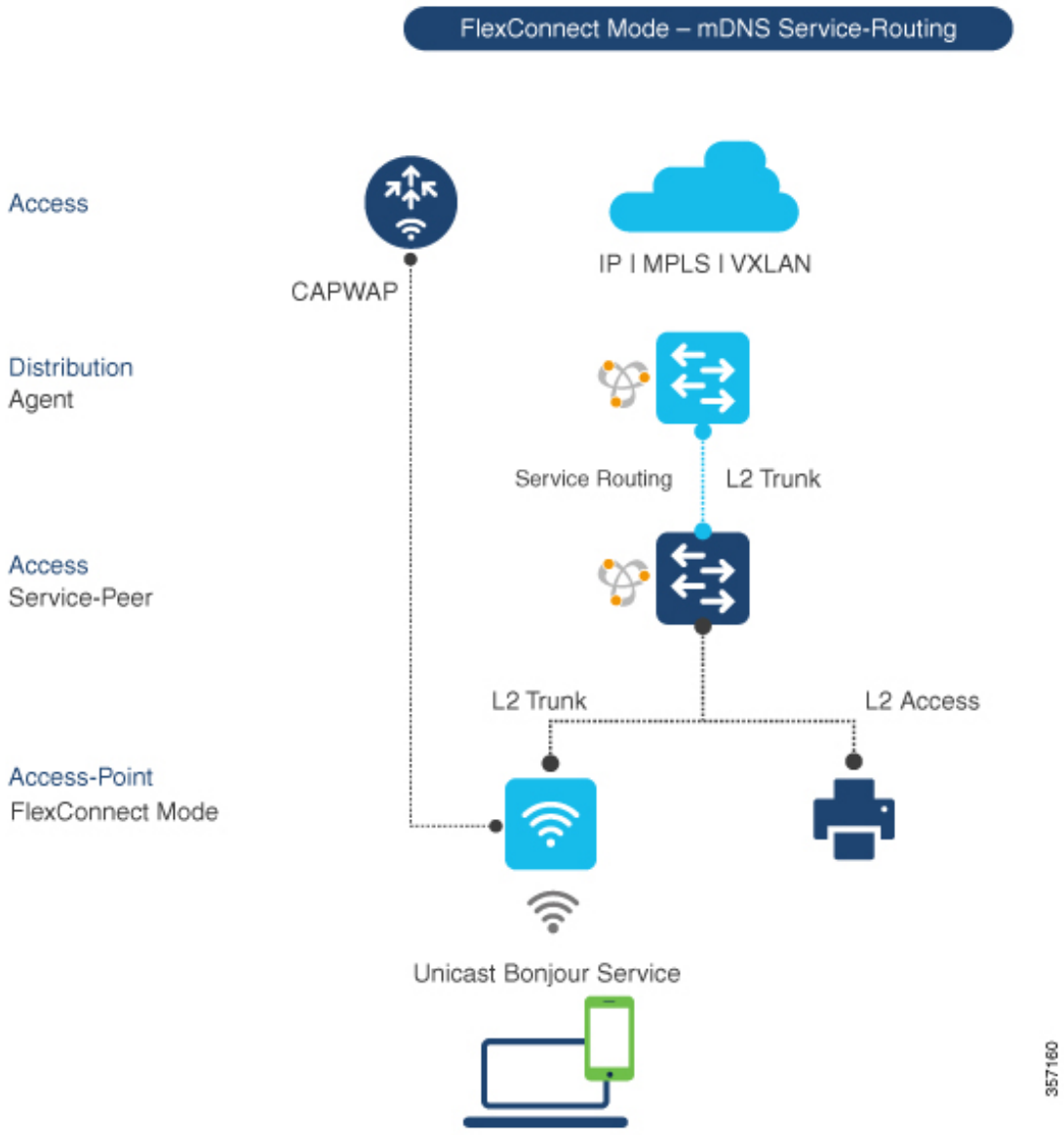
- **AP Based mDNS Gateway**—The Cisco FlexConnect mode wireless access points can alternatively be implemented as mDNS gateway when connected to unsupported LAN access switch. In this method, the mDNS service discovery and distribution follows flood-n-learn mechanism over the Layer 2 wireless network. To implement AP based mDNS gateway, see the Multicast Domain Name System chapter.

Understanding Local Area Bonjour for Wireless FlexConnect Mode

The controller supports mDNS gateway function with various advancements for broad range of wireless networks. As the enterprise requirements expands it drives IT organization to introduce new network deployment models, supporting mobile devices and distributed zero-configuration services following increased scale, granular security control and resiliency for mission critical networks. The common unified Cisco IOS-XE operating system across Cisco Catalyst 9000 series LAN switches and Cisco Catalyst 9800 series controller enables distributed Bonjour gateway function at network edge. With end-to-end Wide Area Bonjour service-routing, the new solution enables service-oriented enterprise networks with intuitive user-experience.

The following figure illustrates how the controller connected to wireless access points support mDNS gateway function to wireless users in FlexConnect Local Switching mode.

Figure 75: Cisco Catalyst 9800 Series Controller Local Area Bonjour for Wireless - FlexConnect Mode



The Cisco Catalyst 9000 series switches in the Layer 2 access layer and Layer 3 distribution layer must be configured in the following mDNS gateway mode to enable Unicast-based mDNS service-routing between wired and FlexConnect Local Switching mode wireless users within the same Layer 2 network block:

- **Service-Peer** - The Layer 2 access switch connecting wireless access point in FlexConnect Local Switching mode must be configured with mDNS gateway in Service-Peer mode. Each Layer 2 access switch provides mDNS gateway function between locally attached wired and FlexConnect mode wireless users. The Unicast-based mDNS service discovery and distribution within same or different VLANs is supported with bi-directional mDNS policies on single Layer 2 access switch.
- **SDG Agent** - The mDNS flood-n-learn based method in Layer 2 network is replaced with simple Unicast based service-routing between Layer 2 access switch in Service-Peer mode and upstream distribution-layer

in mDNS gateway SDG Agent mode. The Unicast based mDNS service-routing eliminates mDNS flood over Layer 2 trunk ports providing increased bandwidth, enhanced security, location-based services, and flood control management in wired and FlexConnect wireless network.

Configuring Local Area Bonjour for Wireless FlexConnect Mode

This section provides configuration guidelines to implement Cisco Catalyst 9000 series Ethernet switch as mDNS gateway and enable service-peer and SDG Agent mode to enable service-routing with upstream distribution-layer Cisco Catalyst 9000 series switch in SDG Agent mode to build Local Area Bonjour.

Configuring mDNS Gateway Mode (CLI)

To enable mDNS gateway and Service-Peer mode on Layer 2 access switch and SDG Agent mode on Layer 3 distribution layer switch, perform the following:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS on the Layer 2 Catalyst switch and enters the mDNS gateway configuration mode. (Optional) You can configure the following additional parameters: • **air-print-helper**: Enables communication between Apple iOS devices like iPhone or iPad to discover and use older printers that does not support driverless AirPrint function. • **cache-memory-max**: Configures the percentage memory for cache. • **ingress-client**: Configures Ingress client packet tuners. • **rate-limit**: Enables rate limiting of incoming mDNS packets. • **service-announcement-count**: Configures maximum advertisements.

	Command or Action	Purpose
		• **service-announcement-timer**: Configures advertisements announcement timer periodicity. • **service-query-count**: Configures maximum queries. • **service-query-timer**: Configures query forward timer periodicity. • **service-type-enumeration**: Configures service enumeration. **Note** For **cache-memory-max**, **ingress-client**, **rate-limit**, **service-announcement-count**, **service-announcement-timer**, **service-query-count**, **service-query-timer**, and **service-type-enumeration** commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.

Step 4	**mode** {**service-peer** | **sdg-agent**}
	Example:
	`Device(config-mdns-sd)# mode service-peer`
	`Device(config-mdns-sd)# mode sdg-agent`
		Configure mDNS gateway in one of the following modes based on the system settings:
		• **service-peer**– Enables Layer 2 Catalyst access switch in mDNS Service-Peer mode.
		• **sdg-agent**– Default. Enables Layer 3 distribution layer Catalyst switch in SDG Agent mode to peer with central Cisco Catalyst Center controller for Wide Area Bonjour service routing.

Step 5	**exit** **Example:** `Device(config-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

Configuring mDNS Service Policy (CLI)

You need to perform the following to configure an mDNS service policy:

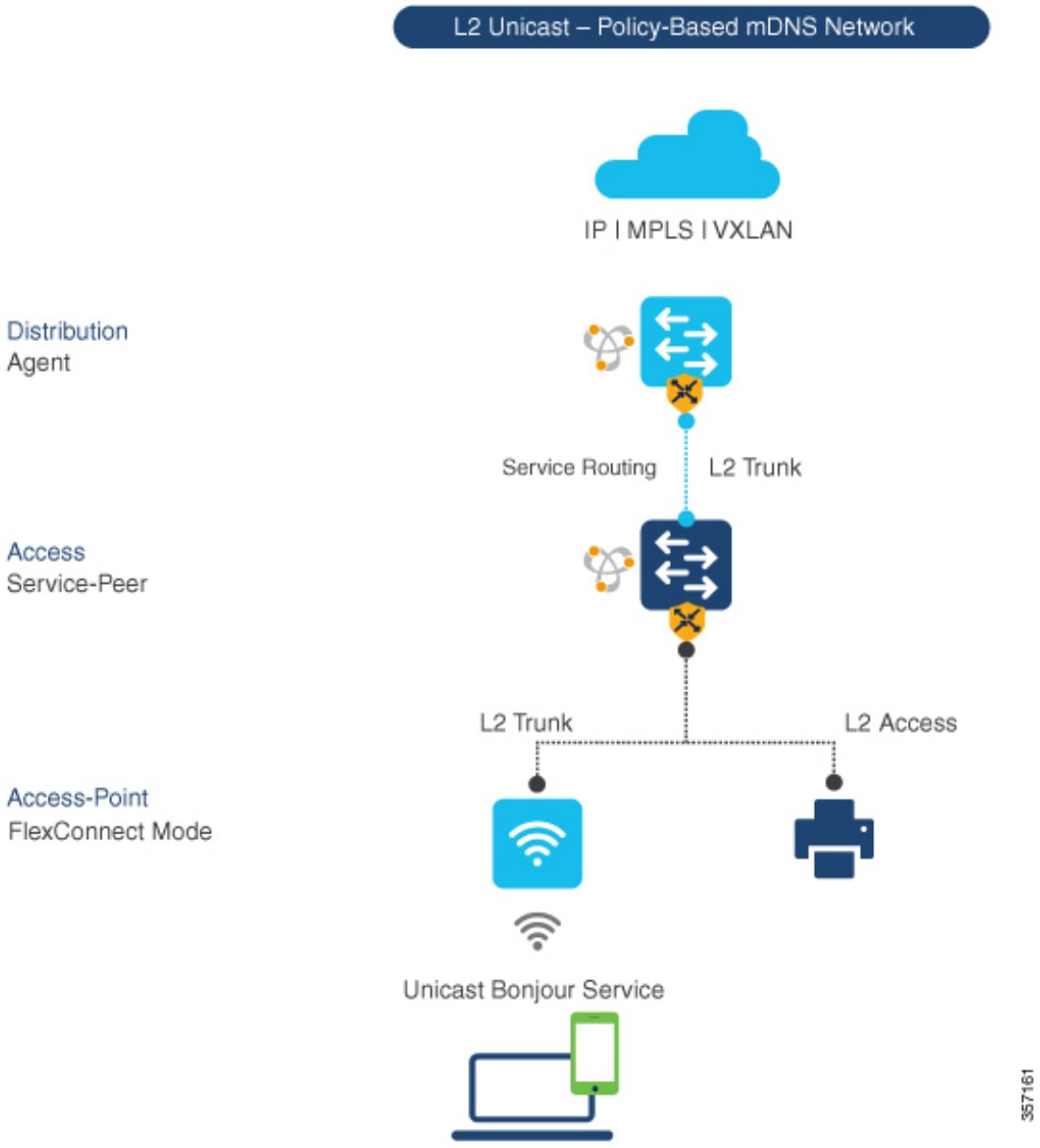
1. Create service-list to permit built-in or user-defined custom service types.

2. Associate service-list to a service-policy to enforce ingress or egress direction.
3. Apply the service policy to the new VLAN configuration mode.

Note You will need this configuration in Service-Peer mode for Layer 2 Catalyst switch and SDG agent mode for Layer 3 Catalyst switch.

The following figure shows how to configure mDNS policies on Catalyst switch in Service-Peer and SDG agent modes.

Figure 76: mDNS Service Policy Configuration on Catalyst Switch in Service-Peer and SDG Agent Modes



This procedure builds and applies service-policies on target VLAN in service-peer and SDG agent modes.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**mdns-sd service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config)# mdns-sd service-list VLAN100-LIST-IN in`
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
		Configure mDNS service-list to classify one or more service types. Unique service-list is required to process incoming mDNS message and outbound response to request locally connected wired or FlexConnect wireless end points.

Step 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
	Example:
	`Device(config)# mdns-sd service-list VLAN100-LIST-IN in`
	`Device(config-mdns-sl-in)# match APPLE-TV`
	`Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`
		Matches inbound service-list.
		The Catalyst switch validates to accept or drop incoming mDNS service-type (such as, Apple TV) advertisement or query matching message type from locally connected wired or FlexConnect wireless end points. The service-list contains implicit deny at the end.
		The default message-type used is **any**.

Step 5	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
	Example:
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
	`Device(config-mdns-sl-in)# match APPLE-TV`
	`Device(config-mdns-sl-in)# match PRINTER-IPPS`
		Matches outbound service-list.
		The Catalyst switch provides local service proxy function by responding matching service-type to the requesting end point(s). For example, the Apple-TV and Printer learnt from VLAN 100 will be distributed to FlexConnect wireless receiver in same VLAN 100. The service-list contains implicit deny at the end.
		The message-type for outbound service-list is not required.

Step 6	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy VLAN100-POLICY`	Creates unique mDNS service-policy in global configuration mode.

Step 7	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config)# mdns-sd service-policy VLAN100-POLICY`
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-IN in`
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-OUT out`
		Configures mDNS service-policy to associate service-list for each direction.

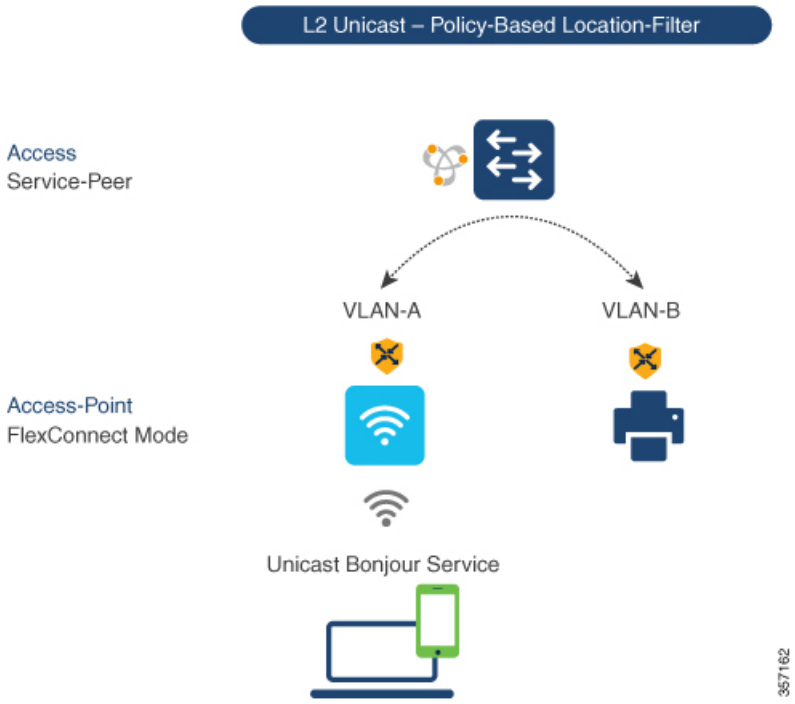
	Command or Action	Purpose
Step 8	**vlan configuration** *ID* **Example:** `Device(config)# vlan configuration 100`	Enables wired or wireless FlexConnect user VLAN configuration for advanced service parameters. One or more VLANs can be created for the same settings. Here, *ID* refers to the VLAN configuration ID. The range is from 101 to 110 and 200. This range allows to configure consecutive and non-consecutive VLAN ID(s).
Step 9	**mdns-sd gateway** **Example:** `Device(config-vlan)# mdns-sd gateway`	Enables mDNS gateway on configured wired or FlexConnect wireless user VLAN ID(s).
Step 10	**service-policy** *service-policy-name* **Example:** `Device(config-vlan-mdns)# service-policy VLAN100-POLICY`	Associates mDNS service-policy to the configured wired or FlexConnect wireless user VLAN ID(s).
Step 11	**exit** **Example:** `Device(config-vlan-mdns)# exit`	Exits mDNS gateway configuration mode.

Configuring mDNS Location-Filter (CLI)

Optionally, you can configure mDNS location-filter to allow service discovery and distribution between locally configured VLAN IDs associated to FlexConnect wireless user networks.

The following figure illustrates and references location-filter policy on Catalyst switch in Service-Peer mode permitting to discover and distribute mDNS services between wired and FlexConnect wireless user VLANs.

Figure 77: Catalyst Service-Peer mDNS Location-Filter Configuration



To enable local service proxy on Cisco Catalyst switch in Service-Peer mode and discover mDNS services between local wired and wireless FlexConnect user VLANs, perform the following:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd location-filter** *location-filter-name* **Example:** `Device(config)# mdns-sd location-filter LOCAL-PROXY`	Configures a unique location-filter in global configuration mode.
Step 4	**match location-group** {**all** | **default** | **ID**} **vlan** [*ID*] **Example:**	Configures the match criteria to mutually distribute the permitted services between grouped VLANs. For example, mDNS services can be discovered and distributed using the

	Command or Action	Purpose
	`Device(config-mdns-loc-filter)# match location-group default vlan 100` `Device(config-mdns-loc-filter)# match location-group default vlan 101`	Unicast mode between wireless FlexConnect user VLAN ID 100 and wired user VLAN ID 101.
Step 5	**mdns-sd service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`	Configures the mDNS service-list to classify one or more service types. The **service-list** configuration is required to process any incoming or outgoing mDNS messages.

Step 6	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
	Example:
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
	`Device(config-mdns-sl-out)# match APPLE-TV location-filter LOCAL-PROXY`
		Associates location-filter to one or more service types to enable local proxy between local VLANs. For example, the Apple-TV learnt from VLAN 100 and VLAN 101 will be distributed to receiver in VLAN 100.
		Note You do not require a **message-type** for the outbound service-list.

Step 7	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy VLAN100-POLICY`	Creates unique mDNS service-policy in global configuration mode.

Step 8	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config)# mdns-sd service-policy VLAN100-POLICY`
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-OUT out`
		Configures mDNS service-policy to associate service-list for each direction.

Step 9	**vlan configuration** *ID* **Example:** `Device(config)# vlan configuration 100`	Enables VLAN configuration for advanced service parameters. You can create one or more VLANs with the same settings. Here, *ID* refers to the VLAN configuration ID. The range is from 101 to 110 and 200. This range allows to configure consecutive and non-consecutive VLAN ID(s).
Step 10	**mdns-sd gateway** **Example:** `Device(config-vlan-config)# mdns-sd gateway`	Enables mDNS gateway on configured VLAN ID(s).
Step 11	**service-policy** *service-policy-name* **Example:**	Associates mDNS service-policy to the configured VLAN ID(s).

	Command or Action	Purpose
	`Device(config-vlan-mdns-sd)# service-policy VLAN100-POLICY`	
Step 12	**exit** **Example:** `Device(config-vlan-mdns-sd)# exit`	Exits mDNS gateway configuration mode.

Configuring Custom Service Definition (CLI)

The Cisco IOS-XE supports mapping of various built-in well-known mDNS service-definition types to key mDNS PTR records and user-friendly names. For example, built-in Apple-TV service-type is associated with _airplay. _tcp.local and _raop. _tcp.local PTR records to successfully enable service in the network. Network administrators create custom service-definition with matching mDNS PTR records to enable end mDNS service-routing in the network.

The custom service-definition can be associated to the service-list as described in the following steps:

Procedure

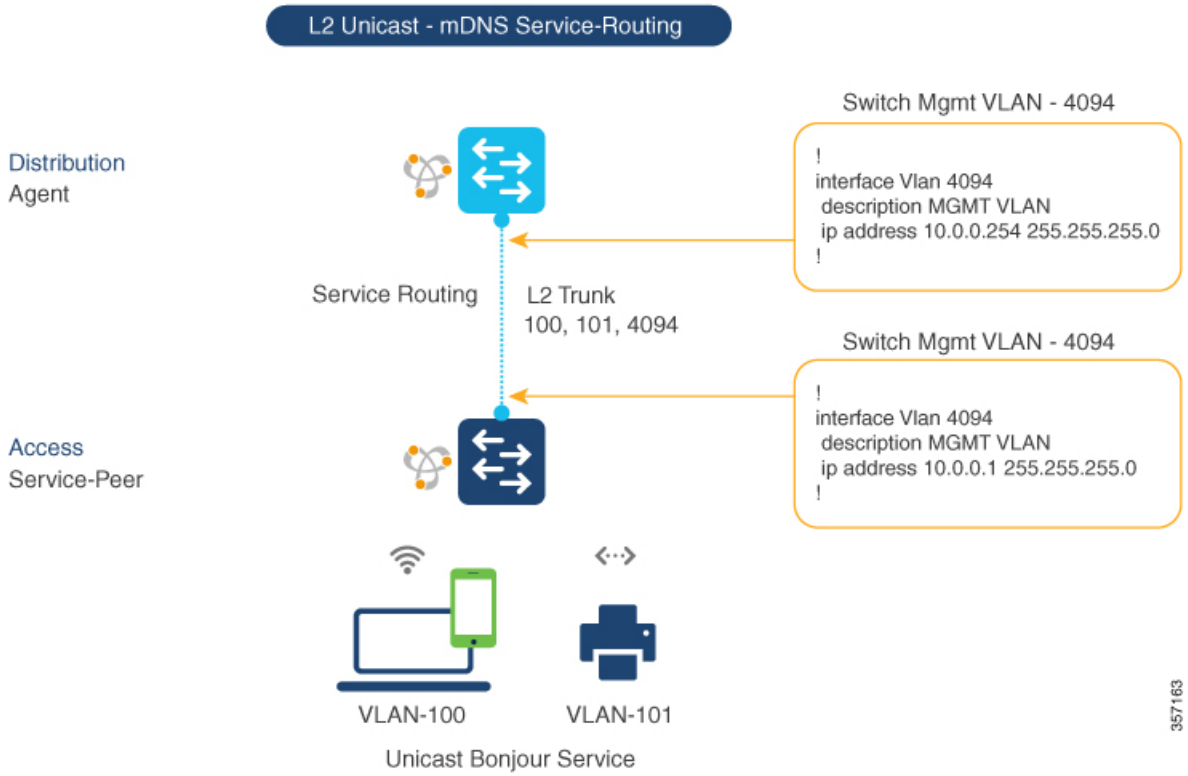
	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition APPLE-CLASSROOM`	Creates a unique service-definition name for custom service-types.
Step 4	**service-type** *custom-mDNS-PTR* **Example:** `Device(config-mdns-ser-def)# service-type _classroom. _tcp.local`	Configures a regular-expression string for custom mDNS PoinTeR(PTR) record.
Step 5	**exit** **Example:** `Device(config-mdns-ser-def)# exit`	Exits mDNS gateway configuration mode.

Configuring Service-Routing on Service-Peer (CLI)

The Layer 2 Cisco Catalyst switch in Service-Peer mode builds a service-routing with an upstream distribution-layer switch in the SDG Agent mode. To build service-routing, the Layer 2 Cisco Catalyst switch requires at least one interface with valid IP address to reach the upstream SDG Agent Catalyst switch. The switch management port is unsupported.

The following figure illustrates the topology to enable unicast-based service-routing over Layer 2 trunk between access-layer Catalyst switch in the Service-Peer mode and distribution-layer Catalyst switch in SDG Agent mode.

Figure 78: Catalyst Service-Peer Service-Routing Configuration



To enable service-routing on Cisco Catalyst switch in Service-Peer mode and setup mDNS trust interface settings, follow the procedure given below:

Procedure

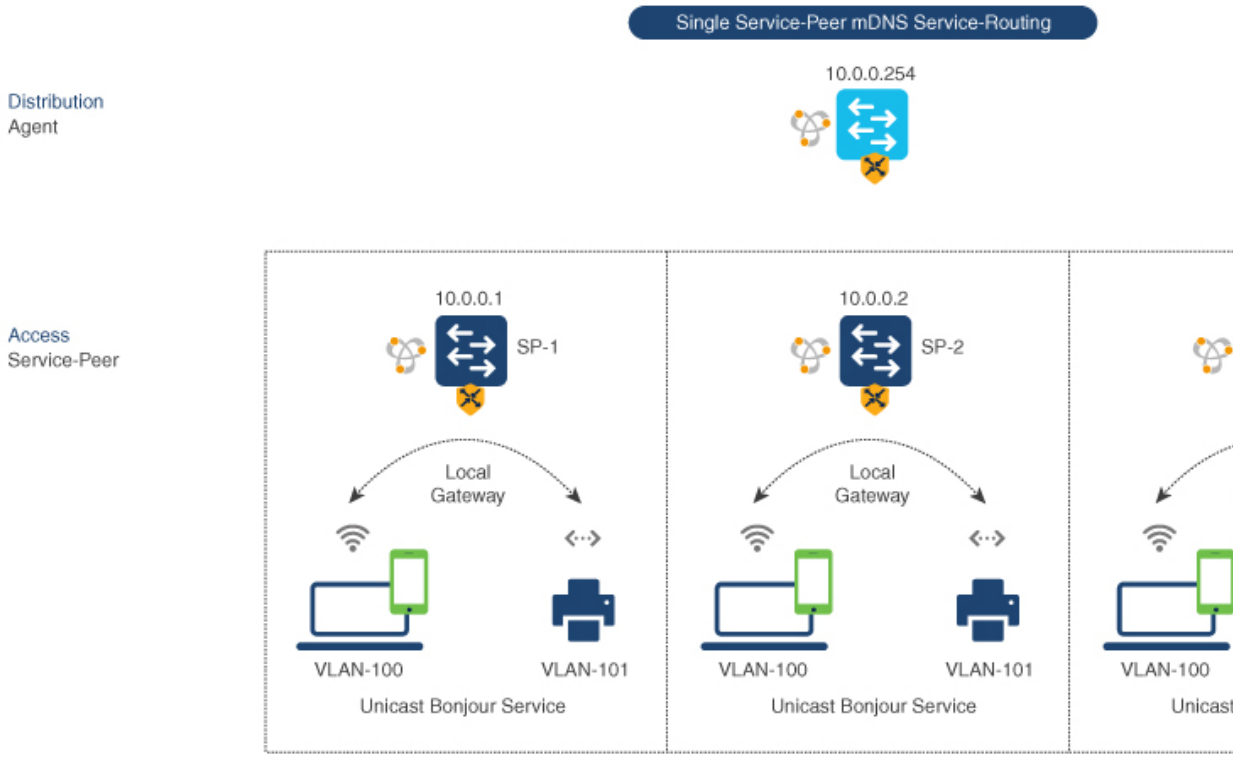
	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables Privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**vlan configuration** *ID* **Example:** `Device(config)# vlan configuration 100`	Enables Wired and FlexConnect user VLAN configuration for advanced service parameters. One or more VLANs can be created for the same settings. Here, *ID* refers to the VLAN configuration ID. For example, *vlan configuration 101-110, 200* range, allows to configure consecutive and non-consecutive VLAN ID(s).
Step 4	**mdns-sd gateway** **Example:** `Device(config-vlan-config)# mdns-sd gateway`	Enables mDNS gateway on configured VLAN ID(s). To enable the respective functionalities, enter the following commands in the mDNS gateway configuration mode: • **active-query timer [sec]**: Configure to enable refresh discovered services and their records with periodic mDNS Query message for permitted service types. The valid range is from 60 to 3600 seconds. The recommended value is 3600 seconds. • **service-mdns-query {ptr | srv | txt}**: Permits processing specific Query type. The default query type is PTR. • **transport {ipv4 | ipv6 | both}**: Permits processing for IPv4, IPv6, or both. It is recommended to use one network type to reduce redundant processing and respond with the same information over two network types. The default network type is IPv4.
Step 5	**source-interface** *ID* **Example:** `Device(config-vlan-mdns-sd)# source-interface vlan 4094`	Selects the interface with a valid IP address to source service-routing session with the upstream Cisco Catalyst SDG Agent switch. Typically, the management VLAN interface can be used.
Step 6	**sdg-agent** [*IPv4_address*] **Example:** `Device(config-vlan-mdns-sd)# sdg-agent 10.0.0.254`	Configures the SDG Agent IPv4 address, typically, the management VLAN gateway address. If FHRP mode, then use the FHRP virtual IP address of the management VLAN.
Step 7	**exit** **Example:** `Device(config-vlan-mdns-sd)# exit`	Exits the mDNS gateway configuration mode.

Configuring Location-Based mDNS

By default, the Layer 2 Catalyst switch in the Service-Peer mode enables per-switch mDNS discovery and distribution in FlexConnect wireless users attached locally to the switch. This default per-switch location-based mDNS is supported even when the FlexConnect user VLANs may be extended between multiple Layer 2 Catalyst switches for user mobility purpose. The mDNS service-policy configuration SDG Agent is required to accept policy-based mDNS service provider and receiver information from downstream Service-Peer access-layer switch.

Figure 79: Per-Switch Location-Based FlexConnect Configuration



Note Configure the mDNS service policy on the distribution layer SDG Agent switch before proceeding to the next configuration step. For more information, see the Configuring mDNS Service Policy section.

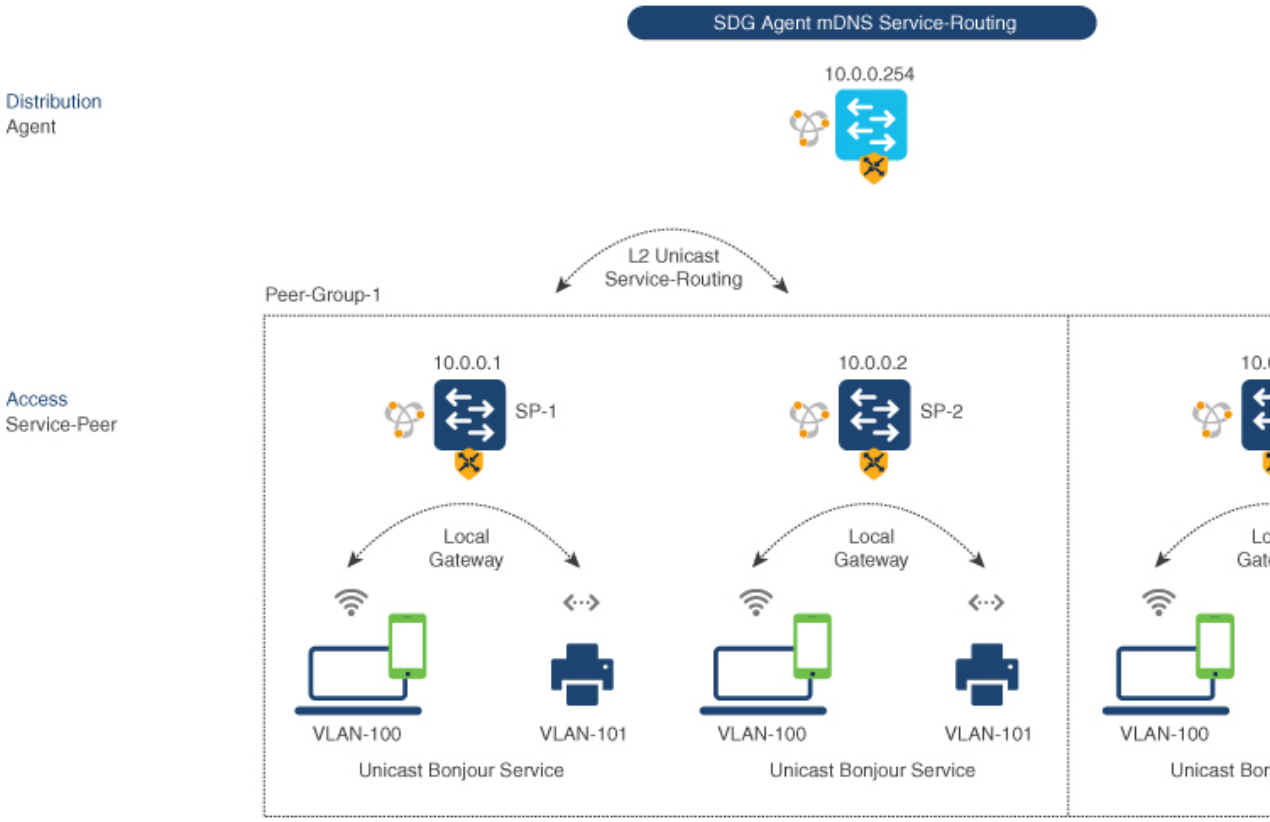
Configuring Service-Routing on SDG Agent (CLI)

The Cisco Catalyst 9000 series switches support SDG Agent mode automatically at the distribution layer and enables Unicast mode Bonjour service-routing with the downstream Layer 2 access-layer Ethernet switches connected to the FlexConnect wireless users. The SDG Agent must be configured with mDNS service-policy on wireless FlexConnect user VLAN to accept mDNS service cache from downstream Service-Peer switches.

This section provides step-by-step configuration guidelines to enable policy-based service discovery and distribution between locally paired Layer 2 access network switches in the Service-Peer mode.

The following figure illustrates unicast service-routing on SDG Agent and downstream Layer 2 access network switches in the Service-Peer mode.

Figure 80: Catalyst SDG Agent Service-Routing Configuration



Note Configure the mDNS service policy on the distribution layer SDG Agent switch before proceeding to the next configuration step. For more information, see the Configuring mDNS Service Policy section.

To enable the mDNS service policy and peer-group on SDG Agent switch, and enable Unicast mode service-routing with Layer 2 access network switches in Service-Peer mode, perform the following:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**mdns-sd service-peer group** *service-peer-group-name* **Example:** `Device(config)# mdns-sd service-peer group group_1`	Configures a unique Service-Peer group.
Step 4	**peer-group** [*ID*] **Example:** `Device(config-mdns-svc-peer)# peer-group 1`	Assigns a unique peer-group ID to the Service-Peers pair permitting mDNS service discovery and distribution within the assigned group list. The valid peer-group range is from 1 to 1000 for each SDG Agent switch.
Step 5	**service-policy** *service-policy-name* **Example:** `Device(config-mdns-svc-peer-grp)# service-policy VLAN100-POLICY`	Associates an mDNS service policy to accept service advertisements and query from the paired Service-Peers.

Step 6	**service-peer** [*IPv4_address*] **location-group** {**all** | **default** | **id**}
	Example:
	`Device(config-mdns-svc-peer-grp)# service-peer 10.0.0.1 location-group default`
	`Device(config-mdns-svc-peer-grp)# service-peer 10.0.0.2 location-group default`
		Configures at least one Service-Peer to accept the mDNS service advertisement or query message. When a group has more than one Service-Peers, the SDG Agent provides Layer 2 Unicast mode routing between the configured peers.
		For example, the SDG Agent provides Unicast based service gateway function between three (10.0.0.1 and 10.0.0.2) Layer 2 Service-Peer switches matching the associated service-policy.
		The mDNS service information from the unpaired Layer 2 Service-Peer (10.0.0.3) cannot announce or receive mDNS services with the other grouped Service-Peers (10.0.0.1 and 10.0.0.2).

Step 7	**exit** **Example:** `Device(config-mdns-svc-peer-grp)# exit`	Exits mDNS gateway configuration mode.

Verifying Local Area Bonjour in Service-Peer Mode

This section provides guidelines to verify various Local Area Bonjour domain mDNS service configuration parameters, cache records, statistics and more on the controller in service-peer mode

Table 151:

Command or Action	Purpose
show mdns-sd cache {all | interface | mac | name | service-peer | static | type | vlan}	Displays available mDNS cache records supporting multiple variables providing granular source details received from wired or wireless FlexConnect user VLANs. The variables are as follows: • all – Displays all available cache records discovered from multiple source connections of a system. • interface – Displays available cache records discovered from the specified Layer 3 interface. • mac - Displays available cache records discovered from the specified MAC address. • name - Displays available cache records based on the service provider announced name. • service-peer - Displays available cache records discovered from the specified Layer 2 Service-Peer. • static – Displays locally configured static mDNS cache entry. • type – Displays available cache records based on the specific mDNS record type, such as, PTR, SRV, TXT, A or AAAA. • vlan - Displays available cache records discovered from the specified Layer 2 VLAN ID in the Unicast mode.
show mdns-sd service-definition {name | type}	Displays built-in and user-defined custom service-definition that maps service name to the mDNS PTR records. The service-definition can be filtered by name or type.
show mdns-sd service-list {direction | name}	Displays inbound or outbound direction list of configured service-list to classify matching service-types for service-policy. The list can be filtered by name or specific direction.
show mdns-sd service-policy {interface | name}	Displays list of mDNS service-policy mapped with inbound or outbound service-list. The service-policy list can be filtered by an associated specified interface or name.

Command or Action	Purpose
show mdns-sd statistics {all | cache | debug | interface | service-list | service-policy | services | vlan}	Displays detailed mDNS statistics processed bi-directionally by the system on each mDNS gateway enabled VLAN configured mDNS in Unicast mode. The expanded keyword for mDNS statistics can provide detailed view on interface, policy, service-list, and services. **Note** This command displays all mDNS packets received from directly connected (Local Mode) or Flex clients in WLAN.
show mdns-sd summary {interface | vlan}	Displays brief information about mDNS gateway and key configuration status on all wired and wireless FlexConnect user VLANs, and interfaces of the system.

Verifying Local Area Bonjour in SDG Agent Mode

This section provides guidelines to verify various Local Area Bonjour domain mDNS service configuration parameters, cache records, statistics and more on the controller in SDG Agent mode

Table 152:

Command or Action	Purpose
show mdns-sd cache {all | interface | mac | name | service-peer | static | type | vlan | vrf}	Displays available mDNS cache records supporting multiple variables providing granular source details. The variables are as follows: • all – Displays all available cache records discovered from multiple source connections of a system. • interface – Displays available cache records discovered from the specified Layer 3 interface. • mac - Displays available cache records discovered from the specified MAC address. • name - Displays available cache records based on the service provider announced name. • service-peer - Displays available cache records discovered from the specified Layer 2 Service-Peer. • static – Displays locally configured static mDNS cache entry. • type – Displays available cache records based on the specific mDNS record type, such as, PTR, SRV, TXT, A or AAAA. • vlan - Displays available cache records discovered from the specified Layer 2 VLAN ID in the Unicast mode. • vrf - Displays per-VRF available cache records based on specific mDNS record type, i.e., PTR, SRV, TXT, A or AAAA.
show mdns-sd service-definition {name | type}	Displays built-in and user-defined custom service-definition that maps service name to the mDNS PTR records. The service-definition can be filtered by name or type.
show mdns-sd service-list {direction | name}	Displays inbound or outbound direction list of the configured service-list to classify matching service-types for service-policy. The list can be filtered by name or specific direction.
show mdns-sd service-policy {interface | name}	Displays list of mDNS service-policy mapped with inbound or outbound service-list. The service-policy list can be filtered by an associated specified interface or name.

Command or Action	Purpose
show mdns-sd statistics {all | cache | debug | interface | service-list | service-policy | services | vlan}	Displays detailed mDNS statistics processed bi-directionally by the system on each mDNS gateway enabled VLAN configured mDNS in Unicast mode. The expanded keyword for mDNS statistics can provide detailed view on interface, policy, service-list, and services.
show mdns-sd summary {interface | vlan}	Displays brief information about mDNS gateway and key configuration status on all VLANs and interfaces of the system.

Reference

Table 153:

Related Topic	Document Title
DNA Service for Bonjour Deployment on Cisco Catalyst 9600 Switch	Cisco Catalyst 9600 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9500 Switch	Cisco Catalyst 9500 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9400 Switch	Cisco Catalyst 9400 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9300 Switch	Cisco Catalyst 9300 Series Switch Software Configuration Guide, Release 17.5.X
Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide	Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide, Release 2.2.2

CHAPTER 195

Configuration Example for Local Mode - Wireless and Wired

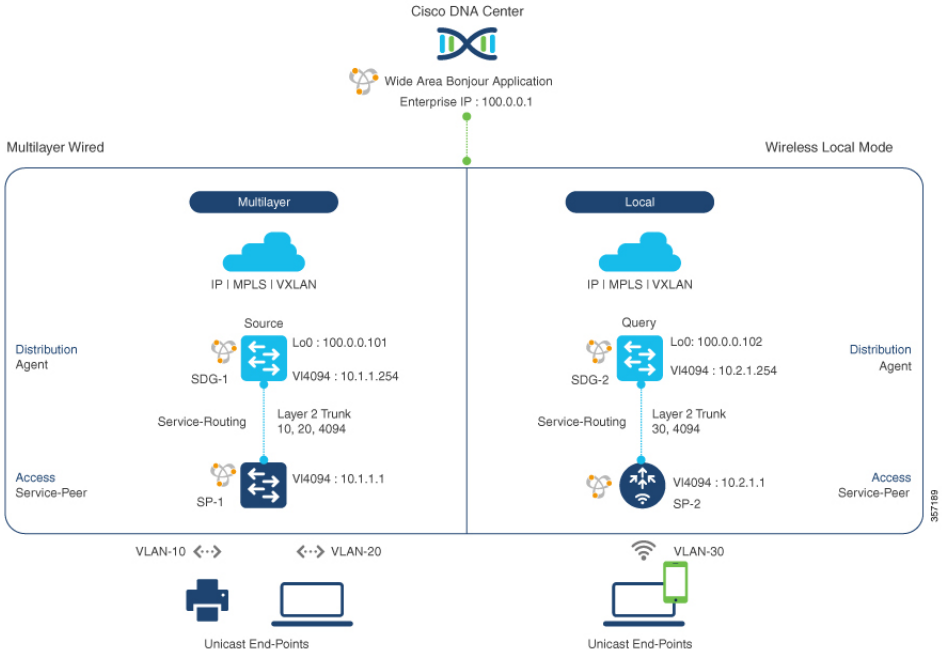
- Overview, on page 2245
- Configuring Wireless AP Multicast Mode, on page 2246
- Configuration Example for Default Service List and Policy in Wide Area Bonjour Between Multilayer Wired and Wireless Endpoints, on page 2247
- Configuration Example for Customized Service List and Policy in Wide Area Bonjour Between Multilayer Wired and Wireless Endpoints, on page 2249
- Cisco Catalyst Center Traditional Multilayer Wired and Wireless Configuration, on page 2252
- Verifying Wide Area Bonjour Between Multilayer Wired and Wireless Local Mode, on page 2254
- Reference, on page 2261

Overview

This chapter provides configuration guidelines to implement Wide Area Bonjour enabling end-to-end policy-based mDNS service discovery and distribution across multilayer wired and wireless local mode. The first hop mDNS gateway at Layer 2 access switch and the controller must be implemented in service peer mode and paired with LAN and wireless distribution-layer switch in SDG agent role. The network-wide distributed SDG agent must be paired with the Cisco Catalyst Center to enable mDNS service-routing across IP core network based on multiple services and network attributes.

The following figure illustrates unicast mode bonjour network environment with AirPrint capable printer and user computer (macOS, Microsoft Windows, etc.) connected to same Ethernet switch. The computers and mobile devices of the wireless user are associated to wireless AP in local mode across multi-hop IP boundary from printers.

Figure 81: Wide Area Bonjour Service-Routing Multilayer Wired and Wireless Local Mode



Configuring Wireless AP Multicast Mode

This procedure configures wireless AP multicast on the controller for local mode APs and IP network.

The controller must be configured with unique IP multicast address for wireless AP in local mode to permit mDNS communication across wired and wireless networks.

Step	Controller Service Peer Configuration
Step-1 Enable global IP Multicast on Cisco Catalyst 9800 series controller.	```! wireless multicast !```
Step-2 Configure Wireless AP mode to Multicast with unique IP Multicast address.	```! wireless multicast 239.254.254.1 !```

The following table provides step-by-step IP multicast configuration guidelines on SDG agent (SDG-1 and SDG-2) at the distribution layer network.

Step	Switch SDG Agent Configuration	WLC SDG Agent Configuration
Step-1 Enable IP multicast-routing on distribution layer switches connecting Cisco Wireless Local Mode Access Point and Cisco Wireless LAN Controller.	```! ip multicast-routing ! ```	```! ip multicast-routing ! ```
Step-2 Configure IP PIM Rendezvous-Point (RP) on distribution layer switches.	```! ip pim rp-address 10.150.255.1 ! ```	```! ip pim rp-address 10.150.255.1 ! ```
Step-3 Enable IP PIM on SVI Interface of distribution layer switches connected Cisco Wireless Local Mode Access Point and Cisco WLC Management VLAN.	```! interface Vlan 101 description CONNECTED TO WIRELESS AP – LOCAL MODE ip pim sparse-mode ! ```	```! interface Vlan 4094 description CONNECTED TO WIRELESS MGMT – WLC ip pim sparse-mode ! ```
Step-4 Enable IP PIM on Layer 3 uplink Interface of distribution layer switches connected Cisco Wireless Local Mode Access Point and Cisco WLC Management VLAN.	```! interface range FortyGigabitEthernet 1/1/1 – 2 description CONNECTED TO IP CORE NETWORK ip pim sparse-mode ! ```	```! interface range FortyGigabitEthernet 1/1/1 – 2 description CONNECTED TO IP CORE NETWORK ip pim sparse-mode ! ```

Note IP Multicast must be enabled in the Layer 3 core network to allow Cisco wireless APs in local mode to successfully join the WLC announced multicast group. For more information, refer to the Cisco online documentation to implement IP multicast networks.

Configuration Example for Default Service List and Policy in Wide Area Bonjour Between Multilayer Wired and Wireless Endpoints

This section provides guidance on configuring Service-Peer, SDG Agent, and Cisco Catalyst Center, allowing the wired and wireless endpoints to dynamically discover default service list using Layer 2 unicast and policy.

Example: Wired and Wireless Access Layer Service Peer Configuration

The following table provides a sample configuration of wired and wireless controller access layer service peer.

Table 154: Configuring Wired and Wireless Access Layer Service Peer

Configuration Step	Sample Configuration: SP-1 Service-Peer Configuration	Sample Configuration: SP-2 Service-Peer Configuration
Step-1: Enable mDNS gateway and set the gateway mode. **Note** In wireless controller, service peer mode is enabled by default with mDNS gateway configuration.	```! mdns-sd gateway mode service-peer ! ```	```! mdns-sd gateway mode service-peer ! ```
Step-2: Activate unicast mDNS gateway and attach service policy on wired VLAN and wireless FlexConnect user VLAN of SP-1 and SP-2 Layer 2 access switch.	```! vlan configuration 10, 30 mdns-sd gateway service-policy LOCAL-AREA-POLICY active-query timer 3600 ! ```	```! vlan configuration 20, 30 mdns-sd gateway service-policy LOCAL-AREA-POLICY active-query timer 3600 ! ```
Step-3: Enable unicast service routing between wired and wireless service peer and SDG agent using wired management source VLAN ID and IP address.	```vlan configuration 10, 30 mdns-sd gateway source-interface vlan 4094 sdg-agent 10.1.1.254 ! ```	```! vlan configuration 20, 30 mdns-sd gateway source-interface vlan 4094 sdg-agent 10.1.1.254 ! ```

Example: Wired and Wireless Distribution Layer SDG Agent Configuration

The following table provides a sample configuration of distribution layer SDG agent.

Table 155: Configuring Wired and Wireles Distribution Layer SDG Agent

Configuration Step	Sample Configuration: SDG-1 – SDG Agent
Step-1: Enable mDNS gateway and set the gateway mode. The default mode is sdg-agent.	```! mdns-sd gateway ! ```
Step-2: Activate unicast mDNS gateway on wired VLAN and wireless user VLAN on SDG agents.	```! vlan configuration 10, 20, 30 mdns-sd gateway ! ```
Step-3: Configure the service peer-group and attach service-policy on the SDG agent distribution switch and enable service-routing between the assigned Service Peer switch group.	```! mdns-sd service-peer group peer-group 1 service-policy LOCAL-AREA-POLICY service-peer 10.1.1.1 location-group default service-peer 10.1.1.2 location-group default ! ```

Configuration Step	Sample Configuration: SDG-1 – SDG Agent
Step-4: Associate outbound service-list to a unique service-policy.	```! mdns-sd service-policy WIDE-AREA-POLICY service-list WIDE-AREA-SERVICES-OUT ! ```
Step-5: Enable Wide Area Bonjour service-routing with service export configuration association controller IP Address, source interface for stateful connection, and mandatory egress policy for Wide Area service-routing.	```! service-export mdns-sd controller DNAC-CONTROLLER-POLICY controller-address 100.0.0.1 controller-source-interface LOOPBACK 0 controller-service-policy WIDE-AREA-POLICY ! ```

Configuration Example for Customized Service List and Policy in Wide Area Bonjour Between Multilayer Wired and Wireless Endpoints

This section provides guidance on configuring Service-Peer, SDG Agent and Cisco Catalyst Center, allowing the wired and wireless endpoints to dynamically discover printer using Layer 2 unicast and policy.

Example: Wired and Wireless Access Layer Service Peer Configuration

The following table provides a sample configuration of wired and wireless controller access layer service peer.

Table 156: Configuring Wired and Wireless Access Layer Service Peer

Configuration Step	Sample Configuration: Switch Service Peer	Sample Configuration: Wireless Controller Service Peer
Step-1: Enable mDNS gateway and set the gateway mode. **Note** In wireless controller, service peer mode is enabled by default with mDNS gateway configuration.	```! mdns-sd gateway mode service-peer ! ```	```! mdns-sd gateway ! ```
Step-2: Create unique mDNS inbound policy to permit ingress AirPrint service announcement on the Catalyst Switch and wireless controller in service peer mode.	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipp ! ```	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipp ! ```

Configuration Step	Sample Configuration: Switch Service Peer	Sample Configuration: Wireless Controller Service Peer
Step-3: Create unique mDNS outbound policy to permit egress AirPrint service response on the Catalyst Switch and wireless controller in service peer mode	! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipp !	! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipp !
Step-4: Associate inbound and outbound service list to a unique service policy.	! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT !	mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT !
Step-5: Activate unicast mDNS gateway and attach service policy on wired VLAN and WLAN. • **Switch**: Activate mDNS gateway per VLAN. • **Controller**: Activate mDNS gateway per WLAN policy profile and SSID	! vlan configuration 10, 20 mdns-sd gateways service-policy LOCAL-AREA-POLICY active-query timer 3600 !	! wireless profile policy WLAN-PROFILE shutdown mdns-sd service-policy LOCAL-AREA-POLICY no shutdown ! wlan WLAN-PROFILE 1 blizzard shutdown mdns-sd-interface gateway no shutdown !
Step-6: (Optional) Enable service routing on wired service peer mDNS between local VLANs. Also, enable location-based wireless service on the controller. • **Switch**: Configure location filter group to discover and distribute between paired local VLAN. • **Controller**: Configure wireless location-based services.	! mdns-sd location-filter LOCAL-PROXY match location-group default vlan 10 match location-group default vlan 20 ! mdns-sd service-list LOCAL-AREA-SERVICES-OUT OUT match printer-ipps location-filter LOCAL-PROXY !	! mdns-sd service-policy LOCAL-AREA-POLICY location ap-location !

Configuration Step	Sample Configuration: Switch Service Peer	Sample Configuration: Wireless Controller Service Peer

Step-7: Enable unicast service routing between wired and wireless service peer and SDG agent.
• **Switch**: Configure SDG agent IP and wired management source VLAN ID and IP address.
• **Controller**: Configure SDG Agent IP and wireless management source VLAN ID and IP address.
	`vlan configuration 10, 20`
	` mdns-sd gateways`
	`  source-interface vlan 4094`
	`  sdg-agent 10.1.1.254`
	`!`
		`!`
		`mdns-sd gateway`
		`  source-interface vlan 4094`
		`  sdg-agent 10.2.1.254`
		`!`

Example: Wired and Wireless Distribution Layer SDG Agent Configuration

The following table provides a sample configuration of distribution layer SDG agent.

Table 157: Configuring Distribution Layer SDG Agent

Configuration Step	Sample Configuration: Wired SDG Agent	Sample Configuration: Wireless SDG Agent

Step-1: Enable mDNS gateway and set the gateway mode.	`!`
	`mdns-sd gateway`
	`!`
		`!`
		`mdns-sd gateway`
		`!`

Step-2: Activate unicast mDNS gateway on wired VLAN and wireless user VLAN on respective SDG agents.	`!`
	`vlan configuration 10, 20`
	` mdns-sd gateway`
	`!`
		`!`
		`vlan configuration 30`
		` mdns-sd gateway`
		`!`

Step-3: Create unique controller bound mDNS policy to permit egress AirPrint service discovery and distribution from Catalyst Switch in SDG agent mode. Inbound policy towards controller is not required.	`!`
	`mdns-sd service-list`
	`WIDE-AREA-SERVICES-OUT out`
	` match printer-ipp`
	`!`
		`!`
		`mdns-sd service-list`
		`WIDE-AREA-SERVICES-OUT out`
		` match printer-ipp`
		`!`

Step-4: Associate outbound service-list to a unique service-policy.	`!`
	`mdns-sd service-policy`
	`WIDE-AREA-POLICY`
	` service-list`
	`WIDE-AREA-SERVICES-OUT`
	`!`
		`!`
		`mdns-sd service-policy`
		`WIDE-AREA-POLICY`
		` service-list`
		`WIDE-AREA-SERVICES-OUT`
		`!`

Configuration Step	Sample Configuration: Wired SDG Agent	Sample Configuration: Wireless SDG Agent
Step-5: Enable Wide Area Bonjour service-routing with service export configuration association controller IP Address, source interface for stateful connection and mandatory egress policy for Wide Area service-routing.	! service-export mdns-sd controller DNAC-CONTROLLER-POLICY controller-address 100.0.0.1 controller-source-interface LOOPBACK 0 controller-service-policy WIDE-AREA-POLICY !	! service-export mdns-sd controller DNAC-CONTROLLER-POLICY controller-address 100.0.0.1 controller-source-interface LOOPBACK 0 controller-service-policy WIDE-AREA-POLICY !

Cisco Catalyst Center Traditional Multilayer Wired and Wireless Configuration

Configuring Service Filters for Traditional Multilayer Wired and Wireless - Local Mode (GUI)

This procedure implements global service filters, which permit the Cisco Wide Area Bonjour application to dynamically discover and distribute service information between trusted Cisco Catalyst SDG agent switches across the IP network.

Procedure

Step 1 Navigate to the **Configuration** tab in the Wide Area Bonjour application.

Step 2 From the sidebar, select the subdomain for which you want to create the service filter.

Step 3 Check the **Service Filter** box.

Step 4 Click **Service Filter** icon from the topology to view a list of the service filters for the selected domain. You can also manually edit existing service filters from this list.

Step 5 Click **Create Service Filter**.

Step 6 From the **Network Mode** drop-down list, choose **Traditional** (the default mode).

Step 7 Enter a unique name for the service filter.

Step 8 (Optional) Enter a description for the service filter.

Step 9 Select one or more service types to permit announcements and queries.

Step 10 Enable or disable service filters after creating them. By default, service filters are enabled.

Configuring Source SDG Agents in Traditional Multilayer Wired and Wireless - Local Mode (GUI)

This procedure configures discovery of wired printer sources from the LAN distribution switches paired with Layer 2 Catalyst Switches in a service peer role. The wireless distribution switches paired with a controller in a service peer role receive query responses for wired printers and distribute the responses to querying devices over the wireless local mode network.

Procedure

Step 1 Click **Add** in the upper-right portion of the Catalyst Center Policy screen.

Step 2 Select the **Query SDG agent** radio button. By default, the **Source** radio button is selected.

Step 3 From the **SDG Agent/IP** drop-down list, select an SDG agent (100.0.0.101) which announces the services, for example, Printer.

Step 4 Select **Peer** from the **Service Layer** drop-down list.

Step 5 Uncheck the box **Any**. By default, this is enabled.

Step 6 Select the query **VLAN** (Vlan-10) to distribute services (Printer) from a specific network.

Step 7 Enable or disable services from the selected query IPv4 subnet. By default, this is enabled.

Step 8 Enable or disable services from the selected query IPv6 subnet. By default, this is enabled.

Step 9 Enter the **service peer IPv4 address** (10.1.1.1).

Step 10 Click the + icon to add more service peers, if any. Select **Any** to accept services from any peer on a selected VLAN.

Step 11 (Optional) Click **Add Next** to add more source SDG agents. (Repeat the preceding steps.)

Step 12 Click **DONE**.

Step 13 Click **CREATE**.

Configuring Query SDG Agents in Traditional Multilayer Wired and Wireless - Local Mode (GUI)

This procedure configures distributed services to query SDG agents connected to a controller in service peer mode, based on a policy.

Procedure

Step 1 Click **Add** in the upper-right portion of the DNA-Center Policy screen.

Step 2 Select the **Query SDG agent** radio button. By default, the **Source** radio button is selected.

Step 3 From the **SDG Agent/IP** drop-down list, select an SDG agent (100.0.0.102) that receives queries for the services (Printer).

Step 4 Select **Peer** from the **Service Layer** drop-down list.

Step 5 Uncheck the box **Any**. By default, this is enabled.

Step 6 Select the query **VLAN** (Vlan-30) to distribute services (Printer) to a specific network.

Step 7 Enable or disable services from the selected query IPv4 subnet. By default, this is enabled.

Step 8 Enable or disable services from the selected query IPv6 subnet. By default, this is enabled.

Step 9 Enter the **service peer IPv4 address** (10.2.1.254).

Step 10 Click the + icon to add more service-peers, if any. Select **Any** to accept services from any peer on a selected VLAN.

Step 11 (Optional) Click **Add Next** to add more query agents. (Repeat the preceding steps.)

Step 12 Click **DONE**.

Step 13 Click **CREATE**.

Verifying Wide Area Bonjour Between Multilayer Wired and Wireless Local Mode

This section provides step-by-step mDNS configuration and service discovery and distribution status based on applied policy on Wired Layer 2 access switch in service peer and SDG agent mode.

Verifying Wired Service-Peer Configuration

Use the following commands on the Cisco Catalyst switch in service peer (SP-1) mode to determine the operational status after applying configuration and discovering the AirPrint service from the local network.

```
Device# show mdns-sd summary vlan 10

VLAN: 10
========================================
mDNS Gateway: Enabled
mDNS Service Policy: LOCAL-AREA-POLICY
Active Query: Enabled
            : Periodicity 3600 Seconds
Transport Type: IPv4
Service Instance Suffix: Not Configured
mDNS Query Type: ALL
SDG Agent IP: 10.1.1.254
Source Interface: Vlan4094

Device# show mdns-sd service-policy name LOCAL-AREA-POLICY

Service Policy Name Service List IN Name Service List Out Name
================================================================================
LOCAL-AREA-POLICY        LOCAL-AREA-SERVICES-IN      LOCAL-AREA-SERVICES-OUT

Device# show mdns-sd cache vlan 10
```

Name	Type	TTL/ Remaining	Vlan-Id/ Interface-name	MAC Address	RR Record Data
_universal. _sub. _ipp. _tcp.local	PTR	4500/4486	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. _ipp. _tcp.local

Name	Type	TTL/ Remaining	Vlan-Id/ Interface-name	MAC Address	RR Record Data
_ipp. _tcp.local	PTR	4500/4486	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. _ipp. _tcp.local
Bldg-1-FL1-PRN. _ipp. _tcp.local	SRV	4500/4486	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. local
Bldg-1-FL1-PRN.local	A	4500/4486	Vl10	ac18.2651.03fe	10.153.1.1
Bldg-1-FL1-PRN.local	AAAA	4500/4486	Vl10	ac18.2651.03fe	2001:10:153: 1:79: A40C:6BEE: AEEC
Bldg-1-FL1-PRN. _ipp. _tcp.local	TXT	4500/4486	Vl10	ac18.2651.03fe	(451)'txtvers=1"priority=EPSON WF-3620 usb_MFG=EPSON" usb_MDL=W~'~

```
Device# show mdns-sd statistics vlan 10

 mDNS Statistics

 Vl10:
  mDNS packets sent              : 612
     IPv4 sent                   : 612
       IPv4 advertisements sent  : 0
       IPv4 queries sent         : 612
     IPv6 sent                   : 0
       IPv6 advertisements sent  : 0
       IPv6 queries sent         : 0
  Unicast sent                   : 0
  mDNS packets rate limited      : 0
  mDNS packets received          : 42
   advertisements received       : 28
   queries received              : 14
     IPv4 received               : 42
       IPv4 advertisements received: 28
       IPv4 queries received       : 14
     IPv6 received                 : 0
       IPv6 advertisements received: 0
       IPv6 queries received       : 0
  mDNS packets dropped           : 0
  ========================================
  Query Type                     : Count
  ========================================
  PTR                            : 12
  SRV                            : 0
  A                              : 0
  AAAA                           : 0
  TXT                            : 0
  ANY                            : 3
  ================================================
  PTR Name                Advertisement     Query
```

```
================================================
_ipp. _tcp.local           9          4
```

Verifying Wired SDG Agent Configuration and Service-Routing Status

This section provides information on mDNS configuration and service-routing on Wired SDG Agent (SDG-1) with locally attached Layer 2 access switches in Service-Peer (SP-1) mode and with centrally paired Cisco Catalyst Center for Wide Area Bonjour service-routing.

```
Device# show mdns-sd summary vlan 10

VLAN: 10
========================================
mDNS Gateway               : Enabled
mDNS Service Policy        : LOCAL-AREA-POLICY
Active Query               : Disabled
Transport Type             : IPv4
Service Instance Suffix    : Not-Configured
mDNS Query Type            : ALL
SDG Agent IP               : Not-Configured
Source Interface           : Not-Configured
```

```
Device# show mdns-sd cache vlan 10

VLAN: 10
========================================
mDNS Gateway               : Enabled
mDNS Service Policy        : LOCAL-AREA-POLICY
Active Query               : Disabled
Transport Type             : IPv4
Service Instance Suffix    : Not-Configured
mDNS Query Type            : ALL
SDG Agent IP               : Not-Configured
Source Interface           : Not-Configured
```

Name	Type	TTL/ Remaining	Vlan-Id /Interface-name	MAC Address	RR Record Data
_universal. _sub._ipp ._tcp.local	PTR	4500/4500	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. _ipp. _tcp.local
_ipp. _tcp.local	PTR	4500/4500	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. _ipp. _tcp.local
Bldg-1-FL1- PRN. _ipp. _tcp.local	SRV	4500/4500	Vl10	ac18.2651.03fe	0 0 631 Bldg-1-FL1-PRN. local
Bldg-1-FL1 -PRN.local	A	4500/4500	Vl10	ac18.2651.03fe	10.153.1.1

Name	Type	TTL/ Remaining	Vlan-Id /Interface-name	MAC Address	RR Record Data
Bldg-1-FL1-PRN.local	AAAA	4500/4500	Vl10	ac18.2651.03fe	2001:10:153:1:79:A40C:6BEE:AEEC
Bldg-1-FL1-PRN. _ipp. _tcp.local	TXT	4500/4500	Vl10	ac18.2651.03fe	(451)txtvers=1"priority=30"ty=EPSON WF-3620 Series"usbMG=EPSON"MDL=W~

```
Device# show mdns-sd sp-sdg statistics

                                 One min, 5 mins, 1 hour
Average Input rate (pps)       : 0,       0,       0
Average Output rate (pps)      : 0,       0,       0
 Messages received:
  Query                       : 15796
  ANY query                   : 0
  Advertisements              : 28
  Advertisement Withdraw      : 0
  Interface down              : 0
  Vlan down                   : 0
  Service-peer ID change      : 0
  Service-peer cache clear    : 12
  Resync response             : 6
 Messages sent:
  Query response              : 5975
  ANY Query response          : 0
  Cache-sync                  : 61
  Get service-instance        : 0

Device# show mdns-sd controller detail

Controller: DNAC-Policy
 IP: 100.0.0.1, Dest Port : 9991, Src Port : 42446, State : UP
 Source Interface : Loopback0, MD5 Disabled
 Hello Timer 30 sec, Dead Timer 120 sec, Next Hello 00:00:24
 Uptime 2d05h (17:02:37 UTC Jan 15 2021)
 Service Buffer: Enabled

Service Announcement:
 Filter: DNAC-CONTROLLER-POLICY
 Count 50, Delay Timer 30 sec, Pending Announcement 0, Pending Withdraw 0
 Total Export Count 56, Next Export in 00:00:24

Service Query:
 Query Suppression Enabled
 Query Count 50, Query Delay Timer 15 sec, Pending 0
 Total Query Count 15791, Next Query in 00:00:09
```

Verifying Wireless Service-Peer Configuration and Service Status

The command given below helps determine the operational status after applying configuration and discovering the AirPrint service from the remote network.

```
Device# show mdns-sd summary

mDNS Gateway: Enabled
Mode: Service Peer
Service Announcement Periodicity (in seconds): 30
Service Announcement Count: 50
Service Query Periodicity (in seconds): 15
Service Query Count: 50
Active Response Timer (in seconds): Disabled
ANY Query Forward: Disabled
SDG Agent IP: 10.2.1.254
Source Interface: Vlan4094
Active Query Periodicity (in minutes): 15
Transport Type: IPv4
mDNS AP service policy: default-mdns-service-policy

Device#  show wireless profile policy detailed WLAN-PROFILE | sec mDNS

mDNS Gateway
  mDNS Service Policy name          : LOCAL-AREA-POLICY

Device# show mdns-sd statistics wlan-id 1

mDNS Packet Statistics
------------------------------------------------
mDNS stats last reset time: 01/10/21 21:38:19
mDNS packets sent: 4592
  IPv4 sent: 4592
    IPv4 advertisements sent: 4592
    IPv4 queries sent: 0
  IPv6 sent: 0
    IPv6 advertisements sent: 0
    IPv6 queries sent: 0
  Multicast sent: 0
    IPv4 sent: 0
    IPv6 sent: 0
mDNS packets received: 297
  advertisements received: 80
  queries received: 217
  IPv4 received: 297
    IPv4 advertisements received: 80
    IPv4 queries received: 217
  IPv6 received: 0
    IPv6 advertisements received: 0
    IPv6 queries received: 0
mDNS packets dropped: 297
Query Type Statistics
  PTR queries received: 1720
  SRV queries received: 8
  A query received: 8
  AAAA queries received: 8
  TXT queries received: 97
  ANY queries received: 153
  OTHER queries received: 0

Device# show mdns-sd sp-sdg statistics

mDNS SP Statistics
```

```
last reset time: 01/10/21 21:37:36

  Messages sent:
   Query                       : 12675
   ANY query                   : 0
   Advertisements              : 24
   Advertisement Withdraw            : 0
   Service-peer ID change            : 0
   Service-peer cache clear          : 7
   Resync response                   : 5
  Messages received:
   Query response                    : 4619
   ANY Query response                : 0
   Cache-sync                        : 48
   Get service-instance              : 0

Device# show mdns-sd query-db

MDNS QUERY DB

Client MAC: 4c32. 7593.e3af
  Vlan ID: 30
  Wlan ID: 1
  Location Group ID: 0
    PTR Name(s):
    _ipp. _tcp.local
```

Verifying Wireless SDG Agent Configuration and Service-Routing Status

This section providees information on mDNS configuration and service-routing on Wireless SDG Agent (SDG-2) with locally attached controller in service peer (SP-2) mode and with centrally paired Cisco DNA-Center for Wide Area Bonjour service-routing.

```
Device# show mdns-sd summary vlan 30

VLAN: 30
========================================
mDNS Gateway            : Enabled
mDNS Service Policy     : LOCAL-AREA-POLICY
Active Query            : Disabled
Transport Type          : IPv4
Service Instance Suffix : Not Configured
mDNS Query Type         : ALL
SDG Agent IP            : Not Configured
Source Interface        : Not Configured

Device# show mdns-sd sp-sdg statistics

                              One min, 5 mins, 1 hour
Average Input rate (pps)       :0,       0,          0
Average Output rate (pps)      :0,       0,          0
 Messages received:
  Query                        : 12191
  ANY query                    : 0
  Advertisements               : 0
  Advertisement Withdraw       : 0
  Interface down               : 0
  Vlan down                    : 0
  Service-peer ID change       : 0
  Service-peer cache clear     : 18
  Resync response              : 10
```

```
 Messages sent:
  Query response               : 1975
  ANY Query response           : 0
  Cache-sync                   : 19
  Get service-instance         : 0

Device# show mdns-sd controller detail

Controller: DNAC-Policy
 IP: 100.0.0.1, Dest Port : 9991, Src Port : 42931, State : UP
 Source Interface: Loopback0, MD5 Disabled
 Hello Timer 30 sec, Dead Timer 120 sec, Next Hello 00:00:19
 Uptime 2d05h (17:10:18 UTC Jan 15 2021)
 Service Buffer: Enabled

Service Announcement:
 Filter: DNAC-CONTROLLER-POLICY
 Count 50, Delay Timer 30 sec, Pending Announcement 0, Pending Withdraw 0
 Total Export Count 0, Next Export in 00:00:19

Service Query:
 Query Suppression Enabled
 Query Count 50, Query Delay Timer 15 sec, Pending 0
 Total Query Count 17093, Next Query in 00:00:19
```

Verifying Cisco Catalyst Center Configuration and Service-Routing Status

The Cisco Wide Area Bonjour application supports comprehensive assurance capabilities to manage service-routing with network-wide distributed Cisco Catalyst switches in SDG-Agent role and mDNS services discovered over Wide Area Bonjour domain. The assurance capabilities in Cisco Wide Area Bonjour provides ability to determine service-routing state, mDNS service state and many more information at various levels for day-2 operations, analysis and troubleshooting. Each category serves unique function to manage and troubleshoot Wide Area Bonjour service-routing for day-2 operation.

This sub-section provides brief overview for each category of monitor function:

- **Dashboard**: The landing page of Cisco Wide Area Bonjour application provides key statistics in various formats to quickly determine service-routing health across the network. The network administrator can monitor operational status of service-routing with SDG Agent devices, historical chart of service discovery request, processing and drops from network-wide distributed devices and top five talkers across the network.
- **Sub-Domain 360°**: The network administrator can briefly collect statistics and status counts in 360° view. The left-panel monitoring, and configuration bar is automatically open upon clicking selected sub-domain to verify configured policies, discovered service-instances on per sub domain basis of the configuration section.
- **Monitor**: A comprehensive 3-tier monitoring and troubleshooting function of Cisco Wide Area Bonjour application for various day-2 operations. The detail view of SDG Agent, Service-Instance and advanced Troubleshooting capabilities allows network administrator to manage and troubleshoot Wide Area Bonjour domain with single of glass on Cisco Catalyst Center.

For more information, see Cisco Wide Area Bonjour on Cisco Catalyst Center User Guide, Release 2.1.2 guide. The assurance capabilities and operation details are explained in Monitor the Cisco Wide Area Bonjour Application chapter to manage Cisco Wide Area Bonjour application with various supporting service-routing assurance function.

Reference

Table 158:

Related Topic	Document Title
DNA Service for Bonjour Deployment on Cisco Catalyst 9600 Switch	Cisco Catalyst 9600 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9500 Switch	Cisco Catalyst 9500 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9400 Switch	Cisco Catalyst 9400 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9300 Switch	Cisco Catalyst 9300 Series Switch Software Configuration Guide, Release 17.5.X
Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide	Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide, Release 2.2.2

CHAPTER 196

Configuration Example for FlexConnect Mode - Wireless and Wired

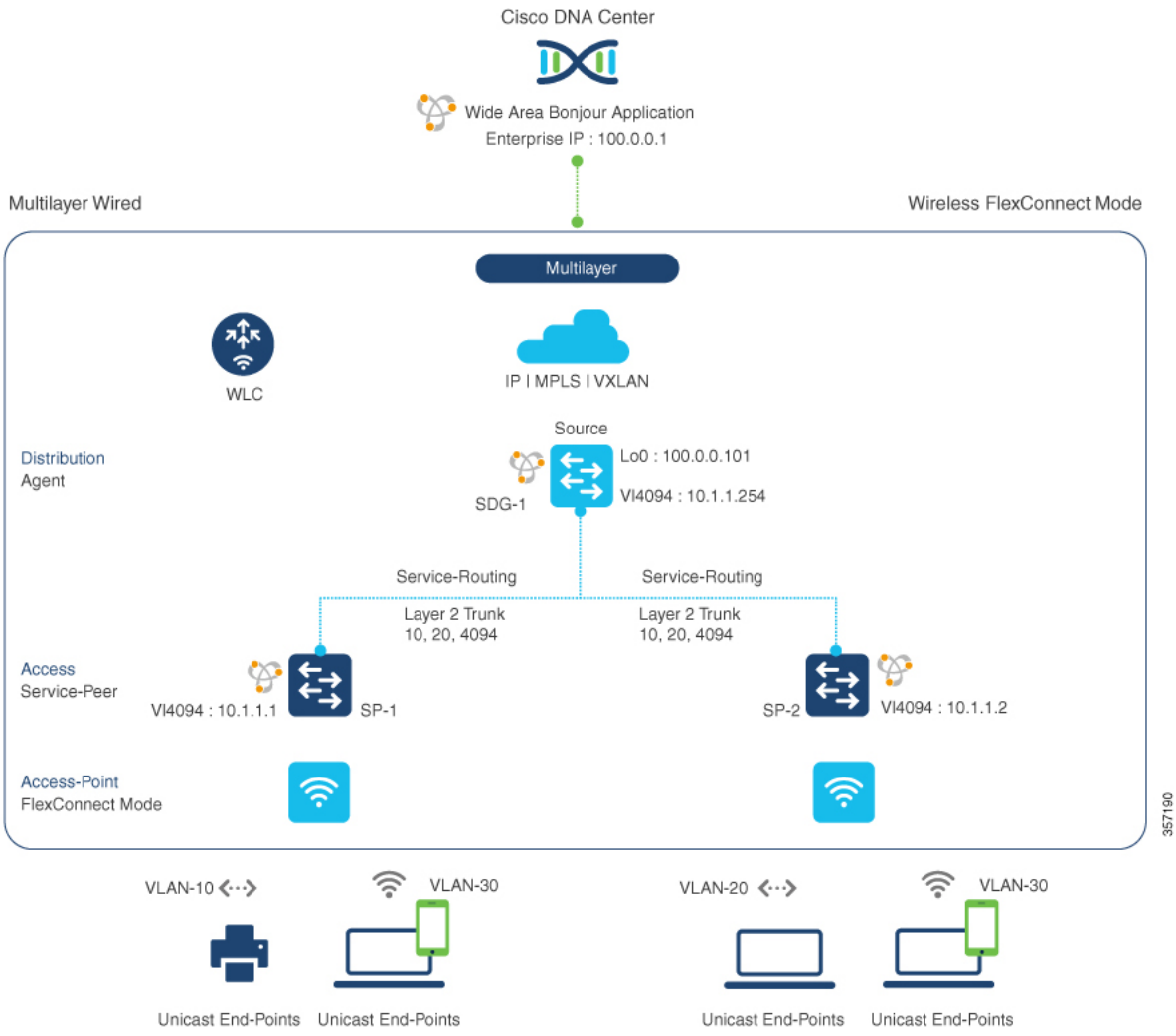
- Overview, on page 2263
- Configuration Example for Default Service List and Policy in FlexConnect Mode - Wireless and Wired, on page 2264
- Configuration Example for Customized Service List and Policy in FlexConnect Mode - Wireless and Wired, on page 2267
- Verifying Configuration Example for FlexConnect Mode - Wireless and Wired, on page 2271
- Reference, on page 2275

Overview

This chapter provides configuration guidelines to implement Local Area Bonjour enabling end-to-end policy-based mDNS service discovery and distribution across multilayer wired and wireless FlexConnect local-switching mode. The first hop mDNS gateway at Layer 2 access switch must be implemented in service peer mode and paired with common distribution-layer switch in SDG agent role IP gateway function to wired and wireless clients. The network-wide distributed SDG agent can be paired alternatively with the Cisco Catalyst Center to enable mDNS service-routing across IP core network providing mDNS service assurance, monitoring and troubleshooting.

The following figure illustrates unicast mode bonjour network environment with AirPrint capable printer and wireless user computer (macOS, Microsoft Windows, and so on.) connected to the same Ethernet switch. The network administrator implements the policy permitting additional endpoints associated to nearby location Ethernet switch to discover and use remote AirPrint capable Printer without flooding mDNS over wired and wireless networks.

Figure 82: Local Area Bonjour Service-Routing Multilayer Wired and Wireless FlexConnect Local-Switching Mode



Configuration Example for Default Service List and Policy in FlexConnect Mode - Wireless and Wired

This section provides guidance on configuring Service-Peer, SDG Agent, and Cisco Catalyst Center, allowing the wired and wireless endpoints to dynamically discover the default service list using Layer 2 unicast and policy.

Example: Wired and Wireless Access Layer Service Peer Configuration

The following table provides a sample configuration of wired and wireless controller access layer service peer.

Table 159: Configuring Wired and Wireless Access Layer Service Peer

Configuration Step	Sample Configuration: SP-1 Service-Peer Configuration	Sample Configuration: SP-2 Service-Peer Configuration
Step-1: Enable mDNS gateway and set the gateway mode.	```! mdns-sd gateway mode service-peer ! ```	```! mdns-sd gateway mode service-peer ! ```
Step-2: Create unique mDNS inbound policy to permit ingress AirPrint service announcement and query on the Catalyst Switch in service peer mode.	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipp ! ```	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipp ! ```
Step-3: Create unique mDNS outbound policy to permit egress AirPrint service response on the Catalyst Switch in service peer mode	```! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipp ! ```	```! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipp ! ```
Step-4: Associate inbound and outbound service list to a unique service policy.	```! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ```	```mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ```
Step-5: Activate unicast mDNS gateway and attach service policy on wired VLAN and wireless FlexConnect user VLAN of SP-1 and SP-2 Layer 2 access switch.	```! vlan configuration 10, 30 mdns-sd gateway service-policy LOCAL-AREA-POLICY active-query timer 3600 ! ```	```! vlan configuration 20, 30 mdns-sd gateway service-policy LOCAL-AREA-POLICY active-query timer 3600 ! ```
Step-6: Enable service routing on wired service peer mDNS between mDNS source and receiver local VLANs. **Note** This step is optional for SP-2 switch as it does not have local mDNS service provider endpoints or VLANs.	```! mdns-sd location-filter LOCAL-PROXY match location-group default vlan 10 match location-group default vlan 30 ! mdns-sd service-list LOCAL-AREA-SERVICES-OUT OUT match printer-ipps location-filter LOCAL-PROXY ! ```	
Step-7: Enable unicast service routing between wired and wireless service peer and SDG agent using wired management source VLAN ID and IP address.	```vlan configuration 10, 30 mdns-sd gateway source-interface vlan 4094 sdg-agent 10.1.1.254 ! ```	```! vlan configuration 20, 30 mdns-sd gateway source-interface vlan 4094 sdg-agent 10.1.1.254 ! ```

Example: Wired and Wireless Distribution Layer SDG Agent Configuration

The following table provides a sample configuration of distribution layer SDG agent.

Table 160: Configuring Wired and Wireless Distribution Layer SDG Agent

Configuration Step	Sample Configuration: SDG-1 – SDG Agent
Step-1: Enable mDNS gateway and set the gateway mode. The default mode is sdg-agent.	```! mdns-sd gateway !```
Step-2: Create a unique mDNS inbound policy to permit ingress AirPrint service announcement and query the Catalyst Switch in Service-Peer mode.	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipp !```
Step-3: Create a unique mDNS outbound policy to permit egress AirPrint service response on Catalyst Switch in Service-Peer mode.	```! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipp !```
Step-4: Associate the inbound and outbound service-list to a unique service-policy.	```! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT !```
Step-5: Activate unicast mDNS gateway on wired VLAN and wireless user VLAN on SDG agents.	```! vlan configuration 10, 20, 30 mdns-sd gateway !```
Step-6: Configure the service peer-group and attach service-policy on the SDG agent distribution switch and enable service-routing between the assigned Service Peer switch group.	```! mdns-sd service-peer group peer-group 1 service-policy LOCAL-AREA-POLICY service-peer 10.1.1.1 location-group default service-peer 10.1.1.2 location-group default !```
Step-7: Create a unique controller bound mDNS policy to permit egress AirPrint service discovery and distribution from Catalyst Switch in SDG agent mode. Inbound policy towards controller is not required.	```! mdns-sd service-list WIDE-AREA-SERVICES-OUT out match printer-ipp !```
Step-8: Associate outbound service-list to a unique service-policy.	```! mdns-sd service-policy WIDE-AREA-POLICY service-list WIDE-AREA-SERVICES-OUT !```

Configuration Step	Sample Configuration: SDG-1 – SDG Agent
Step-9: Enable Wide Area Bonjour service-routing with service export configuration association controller IP Address, source interface for stateful connection, and mandatory egress policy for Wide Area service-routing.	```! service-export mdns-sd controller DNAC-CONTROLLER-POLICY controller-address 100.0.0.1 controller-source-interface LOOPBACK 0 controller-service-policy WIDE-AREA-POLICY ! ```

Configuration Example for Customized Service List and Policy in FlexConnect Mode - Wireless and Wired

This section provides guidance on configuring Service-Peer, SDG Agent, and Cisco Catalyst Center, allowing the wired and wireless endpoints to dynamically discover printer using Layer 2 unicast and policy.

Example: Wired and Wireless Access Layer Service Peer Configuration

The following table provides a sample configuration of wired and wireless controller access layer service peer.

Table 161: Configuring Wired and Wireless Access Layer Service Peer

Configuration Step	Sample Configuration: SP-1 Service-Peer Configuration	Sample Configuration: SP-2 Service-Peer Configuration
Step-1: Enable mDNS gateway and set the gateway mode.	```! mdns-sd gateway mode service-peer ! ```	```! mdns-sd gateway mode service-peer ! ```
Step-2: Create unique mDNS inbound policy to permit ingress AirPrint service announcement and query on the Catalyst Switch in service peer mode.	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipp ! ```	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipp ! ```
Step-3: Create unique mDNS outbound policy to permit egress AirPrint service response on the Catalyst Switch in service peer mode	```! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipp ! ```	```! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipp ! ```
Step-4: Associate inbound and outbound service list to a unique service policy.	```! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ```	```mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ```

Configuration Step	Sample Configuration: SP-1 Service-Peer Configuration	Sample Configuration: SP-2 Service-Peer Configuration
Step-5: Activate unicast mDNS gateway and attach service policy on wired VLAN and wireless FlexConnect user VLAN of SP-1 and SP-2 Layer 2 access switch.	! vlan configuration 10, 30 mdns-sd gateway service-policy LOCAL-AREA-POLICY active-query timer 3600 !	! vlan configuration 20, 30 mdns-sd gateway service-policy LOCAL-AREA-POLICY active-query timer 3600 !
Step-6: Enable service routing on wired service peer mDNS between mDNS source and receiver local VLANs. **Note** This step is optional for SP-2 switch as it does not have local mDNS service provider endpoints or VLANs.	! mdns-sd location-filter LOCAL-PROXY match location-group default vlan 10 match location-group default vlan 30 ! mdns-sd service-list LOCAL-AREA-SERVICES-OUT OUT match printer-ipps location-filter LOCAL-PROXY !	
Step-7: Enable unicast service routing between wired and wireless service peer and SDG agent using wired management source VLAN ID and IP address.	vlan configuration 10, 30 mdns-sd gateway source-interface vlan 4094 sdg-agent 10.1.1.254 !	! vlan configuration 20, 30 mdns-sd gateway source-interface vlan 4094 sdg-agent 10.1.1.254 !

Example: Wired and Wireless Distribution Layer SDG Agent Configuration

The following table provides a sample configuration of distribution layer SDG agent.

Table 162: Configuring Wired and Wireles Distribution Layer SDG Agent

Configuration Step	Sample Configuration: SDG-1 – SDG Agent
Step-1: Enable mDNS gateway and set the gateway mode. The default mode is sdg-agent.	! mdns-sd gateway !
Step-2: Create a unique mDNS inbound policy to permit ingress AirPrint service announcement and query the Catalyst Switch in Service-Peer mode.	! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipp !
Step-3: Create a unique mDNS outbound policy to permit egress AirPrint service response on Catalyst Switch in Service-Peer mode.	! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipp !

Configuration Step	Sample Configuration: SDG-1 – SDG Agent
Step-4: Associate the inbound and outbound service-list to a unique service-policy.	```! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT !```
Step-5: Activate unicast mDNS gateway on wired VLAN and wireless user VLAN on SDG agents.	```! vlan configuration 10, 20, 30 mdns-sd gateway !```
Step-6: Configure the service peer-group and attach service-policy on the SDG agent distribution switch and enable service-routing between the assigned Service Peer switch group.	```! mdns-sd service-peer group peer-group 1 service-policy LOCAL-AREA-POLICY service-peer 10.1.1.1 location-group default service-peer 10.1.1.2 location-group default !```
Step-7: Create a unique controller bound mDNS policy to permit egress AirPrint service discovery and distribution from Catalyst Switch in SDG agent mode. Inbound policy towards controller is not required.	```! mdns-sd service-list WIDE-AREA-SERVICES-OUT out match printer-ipp !```
Step-8: Associate outbound service-list to a unique service-policy.	```! mdns-sd service-policy WIDE-AREA-POLICY service-list WIDE-AREA-SERVICES-OUT !```
Step-9: Enable Wide Area Bonjour service-routing with service export configuration association controller IP Address, source interface for stateful connection, and mandatory egress policy for Wide Area service-routing.	```! service-export mdns-sd controller DNAC-CONTROLLER-POLICY controller-address 100.0.0.1 controller-source-interface LOOPBACK 0 controller-service-policy WIDE-AREA-POLICY !```

Cisco Catalyst Center Traditional Multilayer Wired and Wireless Configuration

Configuring Service Filters for Traditional Multilayer Wired and Wireless FlexConnect Local-Switching Mode (GUI)

This procedure implements global service filters, which permit the Cisco Wide Area Bonjour application to dynamically discover and distribute service information between trusted Cisco Catalyst SDG agent switches across the IP network.

Procedure

Step 1 Navigate to the **Configuration** tab in the Wide Area Bonjour application.

Step 2 From the sidebar, select the sub-domain for which you want to create the service filter.

Step 3 Check the **Service Filter** box.

Step 4 Click **Service Filter** icon from the topology to view a list of the service filters for the selected domain. You can also manually edit existing service filters from this list.

Step 5 Click **Create Service Filter**.

Step 6 From the **Network Mode** drop-down list, choose **Traditional** (the default mode).

Step 7 Enter a unique name for the service filter.

Step 8 (Optional) Enter a description for the service filter.

Step 9 Select one or more service types to permit announcements and queries.

Step 10 Enable or disable service filters after creating them. By default, service filters are enabled.

Configuring Source SDG Agents in Traditional Multilayer Wired and Wireless FlexConnect Local-Switching Mode (GUI)

This procedure configures discovery of wired printer sources from the LAN distribution switches paired with Layer 2 Catalyst Switches in a service peer role. The wireless distribution switches paired with a controller in a service peer role receive query responses for wired printers and distribute the responses to querying devices over the wireless FlexConnect local switching mode network.

Procedure

Step 1 Click **Add** on the upper-right of Cisco Catalyst Center.

Step 2 Click the **Source** radio button to select a source SDG agent. By default, this radio button is selected.

Step 3 From the **SDG Agent/IP** drop-down list, select an SDG agent (100.0.0.101) which announces the services, for example, Printer.

Step 4 Select **Peer** from the **Service Layer** drop-down list.

Step 5 Uncheck the box **Any**. By default, this is unchecked.

Step 6 Select the query **VLAN** (Vlan-10) to distribute services (Printer) from a specific network.

Step 7 Enable or disable services from the selected query IPv4 subnet. By default, this is enabled.

Step 8 Enable or disable services from the selected query IPv6 subnet. By default, this is enabled.

Step 9 Enter the **service peer IPv4 address** (10.1.1.1).

Note Select **Any** to accept services from any peer on a selected VLAN.

Step 10 (Optional) Click **Add Next** to add more source SDG agents. (Repeat the preceding steps.)

Step 11 Click **DONE**.

Step 12 Click **CREATE**.

Configuring Query SDG Agents in Traditional Multilayer Wired and Wireless FlexConnect Local-Switching Mode (GUI)

This procedure configures distributed services to query SDG agents connected to a controller in service peer mode, based on a policy.

If the network environment is different, see the Cisco Wide Area Bonjour on Cisco Catalyst Center User Guide, Release 2.1.2.

Procedure

Step 1 Click **Add** on the upper-right of Cisco Catalyst Center.

Step 2 Select the **Query SDG agent** radio button. By default, the **Source** radio button is selected.

Step 3 From the **SDG Agent/IP** drop-down list, select an SDG agent (100.0.0.102) that receives queries for the services (Printer).

Step 4 Select **Peer** from the **Service Layer** drop-down list.

Step 5 Uncheck the box **Any**. By default, this is enabled.

Step 6 Select the query **VLAN** (Vlan-30) to distribute services (Printer) to a specific network.

Step 7 Enable or disable services from the selected query IPv4 subnet. By default, this is enabled.

Step 8 Enable or disable services from the selected query IPv6 subnet. By default, this is enabled.

Step 9 Enter the **service peer IPv4 address** (10.2.1.254).

Step 10 Click the + icon to add more service-peers, if any. Select **Any** to accept services from any peer on a selected VLAN.

Step 11 (Optional) Click **Add Next** to add more query agents. (Repeat the preceding steps.)

Step 12 Click **DONE**.

Step 13 Click **CREATE**.

Verifying Configuration Example for FlexConnect Mode - Wireless and Wired

This section provides step-by-step mDNS configuration and service discovery and distribution status based on applied policy on Wired Layer 2 access switch in service peer and SDG agent mode.

Verifying Wired Service-Peer Configuration

Use the following commands on the Cisco Catalyst switch in service peer (SP-1 and SP-2) mode to determine the operational status after applying configuration and discovering the AirPrint service from the local network.

```
Device# show mdns-sd summary vlan 10

VLAN: 10
==========================================
mDNS Gateway: Enabled
mDNS Service Policy: LOCAL-AREA-POLICY
```

```
Active Query: Enabled
            : Periodicity 3600 Seconds
Transport Type: IPv4
Service Instance Suffix: Not Configured
mDNS Query Type: ALL
SDG Agent IP: 10.1.1.254
Source Interface: Vlan4094
```

```
Device# show mdns-sd service-policy name LOCAL-AREA-POLICY

Service Policy Name     Service List IN Name     Service List Out Name
================================================================================
LOCAL-AREA-POLICY       LOCAL-AREA-SERVICES-IN    LOCAL-AREA-SERVICES-OUT
```

```
Device# show mdns-sd cache vlan 10
```

Name	Type	TTL/ Remaining	Vlan-Id/ Interface-name	MAC Address	RR Record Data
_universal. _sub. _ipp. _tcp.local	PTR	4500/4486	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. _ipp. _
_ipp. _tcp.local	PTR	4500/4486	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. _ipp. _
Bldg-1-FL1-PRN. _ipp. _tcp.local	SRV	4500/4486	Vl10	ac18.2651.03fe	0 0 631 Bldg-1-FL1-PRN
Bldg-1-FL1-PRN.local	A	4500/4486	Vl10	ac18.2651.03fe	10.153.1.1
Bldg-1-FL1-PRN.local	AAAA	4500/4486	Vl10	ac18.2651.03fe	2001:10:153: 1:79:A40C:
Bldg-1-FL1-PRN. _ipp. _tcp.local	TXT	4500/4486	Vl10	ac18.2651.03fe	(451)'txtvers=1"priority= ty=EPSON WF-3620 Ser usb_MFG=EPSON" usb_MDL=W~'~

```
Device# show mdns-sd statistics vlan 10

 mDNS Statistics

 Vl10:
  mDNS packets sent              : 612
     IPv4 sent                   : 612
       IPv4 advertisements sent  : 0
       IPv4 queries sent         : 612
     IPv6 sent                   : 0
       IPv6 advertisements sent  : 0
       IPv6 queries sent         : 0
  Unicast sent                   : 0
  mDNS packets rate limited      : 0
  mDNS packets received          : 42
   advertisements received       : 28
   queries received              : 14
     IPv4 received               : 42
       IPv4 advertisements received: 28
       IPv4 queries received       : 14
```

```
   IPv6 received                : 0
     IPv6 advertisements received: 0
     IPv6 queries received       : 0
mDNS packets dropped             : 0
=======================================
Query Type                       : Count
=======================================
PTR                              : 12
SRV                              : 0
A                                : 0
AAAA                             : 0
TXT                              : 0
ANY                              : 3
================================================
PTR Name                 Advertisement     Query
================================================
_ipp. _tcp.local           9          4
```

Verifying Wired SDG Agent Configuration and Service-Routing Status

This section provides information on mDNS configuration and service-routing on Wired and Wireless SDG Agent (SDG-1) with locally attached Layer 2 access switches in Service-Peer (SP-1 and SP-2) mode and with centrally paired Cisco Catalyst Center for Wide Area Bonjour service-routing.

```
Device# show mdns-sd summary vlan 10

VLAN: 10
=======================================
mDNS Gateway               : Enabled
mDNS Service Policy        : LOCAL-AREA-POLICY
Active Query               : Disabled
Transport Type             : IPv4
Service Instance Suffix    : Not Configured
mDNS Query Type            : ALL
SDG Agent IP               : Not-Configured
Source Interface           : Not-Configured
```

```
Device# show mdns-sd cache vlan 10
```

Name	Type	TTL/ Remaining	Vlan-Id /Interface-name	MAC Address	RR Record Data
_universal. _sub. _ipp. _tcp.local	PTR	4500/4500	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. _ipp. _tcp.local
_ipp._tcp.local	PTR	4500/4500	Vl10	ac18.2651.03fe	Bldg-1-FL1-PRN. _ipp. _tcp.local
Bldg-1-FL1-PRN. _ipp._tcp.local	SRV	4500/4500	Vl10	ac18.2651.03fe	0 0 631 Bldg-1-FL1-PRN.local
Bldg-1-FL1 -PRN.local	A	4500/4500	Vl10	ac18.2651.03fe	10.153.1.1

Name	Type	TTL/ Remaining	Vlan-Id /Interface-name	MAC Address	RR Record Data
Bldg-1-FL1-PRN.local	AAAA	4500/4500	Vl10	ac18.2651.03fe	2001:10:153:1:79 A40C:6BEE:AEEC
Bldg-1-FL1-PRN._ipp._tcp.local	TXT	4500/4500	Vl10	ac18.2651.03fe	(451)txtvers=1 priority=30 ty=EPSON WF-3620 Series" usb_MFG=EPSON usb_MDL=WF-

```
Device# show mdns-sd sp-sdg statistics

                                One min, 5 mins, 1 hour
Average Input rate (pps)       : 0,       0,       0
Average Output rate (pps)      : 0,       0,       0
 Messages received:
  Query                       : 15796
  ANY query                   : 0
  Advertisements              : 28
  Advertisement Withdraw      : 0
  Interface down              : 0
  Vlan down                   : 0
  Service-peer ID change      : 0
  Service-peer cache clear    : 12
  Resync response             : 6
 Messages sent:
  Query response              : 5975
  ANY Query response          : 0
  Cache-sync                  : 61
  Get service-instance        : 0

Device# show mdns-sd controller detail

Controller: DNAC-Policy
 IP: 100.0.0.1, Dest Port : 9991, Src Port : 42446, State : UP
 Source Interface: Loopback0, MD5 Disabled
 Hello Timer 30 sec, Dead Timer 120 sec, Next Hello 00:00:24
 Uptime 2d05h (17:02:37 UTC Jan 15 2021)
 Service Buffer: Enabled

Service Announcement:
 Filter: DNAC-CONTROLLER-POLICY
 Count 50, Delay Timer 30 sec, Pending Announcement 0, Pending Withdraw 0
 Total Export Count 56, Next Export in 00:00:24

Service Query:
 Query Suppression Enabled
 Query Count 50, Query Delay Timer 15 sec, Pending 0
 Total Query Count 15791, Next Query in 00:00:09
```

Verifying Cisco Catalyst Center Configuration and Service Routing Status

The Cisco Wide Area Bonjour application supports comprehensive assurance capabilities to manage service routing with network-wide distributed Cisco Catalyst switches in SDG Agent role and mDNS services discovered over Wide Area Bonjour domain. The assurance capabilities in Cisco Wide Area Bonjour provides the ability to determine service routing state, mDNS service state, and many more information at various levels for day-2 operations, analysis and troubleshooting. Each category serves unique function to manage and troubleshoot Wide Area Bonjour service routing for day-2 operation.

This sub-section provides brief overview for each category of monitor function:

- **Dashboard**: The landing page of Cisco Wide Area Bonjour application provides key statistics in various formats to quickly determine service routing health across the network. The network administrator can monitor operational status of service routing with SDG Agent devices, historical chart of service discovery request, processing and drops from network-wide distributed devices and top five talkers across the network.
- **Sub-Domain 360°**: The network administrator can briefly collect statistics and status counts in 360° view. The left-panel monitoring, and configuration bar is automatically open upon clicking selected sub-domain to verify configured policies, discovered service-instances on per sub-domain basis of the configuration section.
- **Monitor**: A comprehensive 3-tier monitoring and troubleshooting function of Cisco Wide Area Bonjour application for various day-2 operations. The detail view of SDG Agent, Service-Instance, and advanced Troubleshooting capabilities allows network administrator to manage and troubleshoot Wide Area Bonjour domain with a single pane of glass on Cisco Catalyst Center.

For more information, see Cisco Wide Area Bonjour on Cisco Catalyst Center User Guide, Release 2.1.2 guide. The assurance capabilities and operation details are explained in **Monitor the Cisco Wide Area Bonjour Application** chapter to manage Cisco Wide Area Bonjour application with various supporting service routing assurance function.

Reference

Table 163:

Related Topic	Document Title
DNA Service for Bonjour Deployment on Cisco Catalyst 9600 Switch	Cisco Catalyst 9600 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9500 Switch	Cisco Catalyst 9500 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9400 Switch	Cisco Catalyst 9400 Series Switch Software Configuration Guide, Release 17.5.X
DNA Service for Bonjour Deployment on Cisco Catalyst 9300 Switch	Cisco Catalyst 9300 Series Switch Software Configuration Guide, Release 17.5.X
Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide	Cisco Wide Area Bonjour Application on Cisco Catalyst Center User Guide, Release 2.2.2

PART XIX

Multicast Domain Name System

- Multicast Domain Name System, on page 2279

CHAPTER 197

Multicast Domain Name System

- Introduction to mDNS Gateway, on page 2280
- Guidelines and Restrictions for Configuring mDNS AP, on page 2280
- Enabling mDNS Gateway (GUI), on page 2282
- Enabling or Disabling mDNS Gateway (GUI), on page 2282
- Enabling or Disabling mDNS Gateway (CLI), on page 2283
- Creating Default Service Policy, on page 2284
- Creating Custom Service Definition (GUI), on page 2285
- Creating Custom Service Definition, on page 2285
- Creating Service List (GUI), on page 2286
- Creating Service List, on page 2287
- Creating Service Policy (GUI), on page 2288
- Creating Service Policy, on page 2289
- Configuring a Local or Native Profile for an mDNS Policy, on page 2291
- Configuring an mDNS Flex Profile (GUI), on page 2291
- Configuring an mDNS Flex Profile (CLI), on page 2292
- Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (GUI), on page 2292
- Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (CLI), on page 2293
- Enabling the mDNS Gateway on the VLAN Interface, on page 2293
- Location-Based Service Filtering, on page 2294
- Nearest mDNS-Based Wired Service Filtering, on page 2301
- Configuring mDNS AP, on page 2312
- Enabling mDNS Gateway on the RLAN Interface, on page 2313
- Enabling mDNS Gateway on Guest LAN Interface, on page 2316
- Associating mDNS Service Policy with Wireless Profile Policy (GUI), on page 2317
- Associating mDNS Service Policy with Wireless Profile Policy, on page 2317
- Enabling or Disabling mDNS Gateway for WLAN (GUI), on page 2320
- Enabling or Disabling mDNS Gateway for WLAN, on page 2321
- mDNS Gateway with Guest Anchor Support and mDNS Bridging, on page 2322
- Configuring mDNS Gateway on Guest Anchor, on page 2322
- Configuring mDNS Gateway on Guest Foreign (Guest LAN), on page 2323
- Configuring mDNS Gateway on Guest Anchor, on page 2323
- Configuring mDNS Gateway on Guest Foreign (Guest WLAN), on page 2324
- Verifying mDNS Gateway Configurations, on page 2324

Introduction to mDNS Gateway

Multicast Domain Name System (mDNS) is an Apple service discovery protocol which locates devices and services on a local network with the use of mDNS service records.

The Bonjour protocol operates on service announcements and queries. Each query or advertisement is sent to the Bonjour multicast address ipv4 224.0.0.251 (ipv6 FF02::FB). This protocol uses mDNS on UDP port 5353.

The address used by the Bonjour protocol is link-local multicast address and therefore is only forwarded to the local L2 network. As, multicast DNS is limited to an L2 domain for a client to discover a service it has to be part of the same L2 domain, This is not always possible in any large scale deployment or enterprise.

In order to address this issue, the Cisco Catalyst 9800 Series Wireless Controller acts as a Bonjour Gateway. The controller then listens for Bonjour services, caches these Bonjour advertisements (AirPlay, AirPrint, and so on) from the source or host. For example, Apple TV responds back to Bonjour clients when asked or requested for a service. This way you can have sources and clients in different subnets.

By default, the mDNS gateway is disabled on the controller. To enable mDNS gateway functionality, you must explicitly configure mDNS gateway using CLI or Web UI.

The source IP address of all outgoing mDNS packets use the mDNS source interface VLAN SVI IP address. By default, wireless management interface will be the source interface.

Guidelines and Restrictions for Configuring mDNS AP

- Cisco recommends deploying scalable Wide Area Bonjour to route mDNS service between Wired and Wireless networks. Cisco Catalyst 9800 Series Wireless LAN Controller (WLC) introduces a new mDNS gateway called Service-Peer mode to replace the classic mDNS flood-n-learn to support Enterprise-grade scalable, stateful, and reliable complete unicast-based mDNS service-routing with upstream gateway Cisco Catalyst 9000 Series Switches. For more information, see Cisco DNA Service for Bonjour.
- The mDNS AP (classic flood-n-learn based feature) is enhanced with complete unicast-based service-routing using Cisco Wide Area Bonjour supporting flood-free Wired and Wireless networks to overcome several operational, scalable, and service resiliency challenges.
- The mDNS AP extends the mDNS flood from Wired VLANs to AP and further extends over the CAPWAP tunnel to WLC for central processing across Core network. Cisco recommends that the mDNS AP must be considered only for small network environments.
- The mDNS AP is supported only in Local and Monitor modes. If Cisco Wireless AP is in FlexConnect mode, the Fabric mode AP does not support mDNS AP feature. For more information on how to enable the mDNS service-routing for various distributed Wireless modes, see Cisco DNA Service for Bonjour.
- Wireless users connected to mDNS AP may not be able to browse the Wired mDNS services across flooded Wired VLAN to mDNS AP.
- The Wired mDNS service-provider VLANs must be extended to flood the mDNS traffic up to mDNS AP ethernet port in trunk mode settings. The Wired VLAN extension to mDNS AP may include other Wired flood traffic, such as Broadcast, Unknown Unicast, and Layer 2 Multicast that impacts the mDNS AP scale and performance.

- It is recommended to have minimum one mDNS AP for each Layer 3 Access switch. All Wired mDNS traffic is flooded using alternate L2 methods, if single mDNS AP is shared between multiple Layer 3 Access switch.
- The maximum mDNS AP scale limit for each Cisco Catalyst 9800 Series Wireless LAN Controller (WLC) is limited.
- The maximum mDNS Wired VLAN count for each WLC is limited.
- The old Wired mDNS service entry continues to be advertised to all Wireless users up to 4500 seconds based on the mDNS cache timers on WLC. The stale entries require manual clearing from local cache in WLC.
- The mDNS AP does not support mDNS Query packet suppression or rate-limiter in AP. The Wired mDNS flood from all Wired VLAN is extended to WLC for central processing of policy enforcement.
- The maximum number of flooded packets for each second processing from Wired VLANs to mDNS AP is limited. The mDNS AP performance and reliability may get compromised in large network environments.
- A maximum of 10 Wired VLANs' mDNS flood can be extended to mDNS AP. Combined large Wired VLAN and mDNS AP scale may impact scale and performance in AP and WLC.
- Only one mDNS AP is supported for each Wired VLAN. Multiple mDNS APs cannot be configured to map the same Wired VLAN ID as it causes service instability and duplicate processing.
- High Availability is not supported in multiple mDNS AP. The mDNS services across Wired and Wireless network gets disrupted when connectivity to mDNS AP is lost due to any kinds of failures.
- Only one Wired mDNS service-policy is supported for all network-wide mDNS AP.
- The following limitations hold true when mDNS AP introduces LSS-based mDNS service filtering between flooded Wired VLANs to Wireless:
    - A single mDNS AP with LSS enabled can distribute Wired mDNS services only to nearby limited APs in neighbor list. The Wireless users connected to the non-neighbor list may not be able to discover any Wired mDNS services.
    - Only one mDNS AP can be deployed in each Wired VLAN. The Wired VLANs need to be reconfigured across LAN network to enable unique LSS-based mDNS AP in locations. For instance, to achieve mDNS service discovery in each floor, the Wired VLAN or Subnet must be on each floor with one mDNS AP per floor to discover all other APs as neighbor in the same floor.
- The mDNS AP do not support IPv6 for Wired mDNS service-provider or service-receiver. Only IPv4 is supported.
- The mDNS AP do not support role-based mDNS service filtering between Wired and Wireless networks.
- The mDNS AP do not detect and auto-resolve duplicate mDNS service-instance names across Wired VLANs. The Cisco Catalyst 9800 Series Wireless LAN Controller (WLC) discovers and records the first service instance with unique name in its local cache database. If a duplicate service instance name is discovered, the WLC rejects the duplicate name and does not distribute it to the Wireless clients.
- Wireless multicast link-local is enabled by default. When wireless link-local is enabled, only mDNS Bridging mode is supported. If you require mDNS Gateway for wired services, disable wireless link-local.

- In the mDNS gateway mode, controller does not support service discovery from the mDNS messages using multiple IP fragments.
- If you have a FlexConnect AP as an mDNS gateway, ensure that you do not use "." in the service provider name, as it is not supported.

Enabling mDNS Gateway (GUI)

Procedure

Step 1 Choose **Configuration > Services > mDNS**.

Step 2 In the **Global** section, toggle the slider to enable or disable the **mDNS Gateway**.

Step 3 From the **Transport** drop-down list, choose one of the following types:

- **ipv4**
- **ipv6**
- **both**

Step 4 Enter an appropriate timer value in **Active-Query Timer**. The valid range is between 1 to 120 minutes. The default is 30 minutes.

Step 5 From the **mDNS-AP Service Policy** drop-down list, choose an mDNS service policy.

Note Service policy is optional only if mDNS-AP is configured. If mDNS-AP is not configured, the system uses default-service-policy.

Step 6 Click **Apply**.

Enabling or Disabling mDNS Gateway (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS** > **Global**.

Step 2 Enable or disable the **mDNS Gateway** toggle button.

Step 3 Choose **ipv4** or **ipv6** or **both** from the **Transport** drop-down list.

Step 4 Enter the **Active-Query Timer**.

Step 5 Click **Apply**.

Enabling or Disabling mDNS Gateway (CLI)

Note

- mDNS gateway is disabled by default globally on the controller.
- You need both global and WLAN configurations to enable mDNS gateway.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS gateway.
Step 4	**location** {**ap-location** | **ap-name** | **location-group** | **lss** | **regex** | **site-tag** | **ssid**} **Example:** `Device(config-mdns-sd)# location site-tag`	Filters mDNS gateway based on location. Here, • **ap-location** signifies location-based filtering using AP location. • **ap-name** signifies location-based filtering using AP name. • **location-group** signifies location-based filtering using location group. • **lss** signifies location-based filtering using Location Specific Services (LSS). • **regex** signifies location-based filtering using Regular Expression. • **site-tag** signifies location-based filtering using site tag. • **ssid** signifies location-based filtering using SSID.

	Command or Action	Purpose
		Note The **lss** is the default location filter, if mDNS gateway is configured globally.
Step 5	**transport** {**ipv4** | **ipv6** | **both**} **Example:** `Device(config-mdns-sd)# transport ipv4`	Processes mDNS message on a specific transport. Here, **ipv4** signifies that the IPv4 mDNS message processing is enabled. This is the default value. **ipv6** signifies that the IPv6 mDNS message processing is enabled. **both** signifies that the IPv4 and IPv6 mDNS message is enabled for each network.
Step 6	**active-query timer** *active-query-periodicity* **Example:** `Device(config-mdns-sd)# active-query timer 15`	Changes the periodicity of mDNS multicast active query. **Note** An active query is a periodic mDNS query to refresh dynamic cache. Here, *active-query-periodicity* refers to the active query periodicity in Minutes. The valid range is from 1 to 120 minutes. Active query runs with a default periodicity of 30 minutes.
Step 7	**source-interface vlan** *vlan-id* **Example:** `Device(config-mdns-sd)# source-interface vlan 101`	Configures the source interface to communicate between SDG agent and service peer. By default, wireless management interface is used. The interface that you configure will be used for all mDNS transactions.
Step 8	**exit** **Example:** `Device(config-mdns-sd)# exit`	Returns to global configuration mode.

Creating Default Service Policy

When the mdns gateway is enabled on any of the WLANs by default, mdns-default-service-policy is associated with it. Default service policy consists of default-service-list and their details are explained in this section. You can override the default service policy with a custom service policy.

Procedure

Step 1 Create a service-definition if the service is not listed in the preconfigured services.

Step 2 Create a service list for IN and OUT by using the service-definitions.

Step 3 Use the existing service list to create a new service. For more information, refer to *Creating Service Policy* section.

Step 4 Attach the mdns-service-policy to the profile or VLAN that needs to be enforced.

Step 5 To check the default-mdns-service list, use the following command:

show mdns-sd default-service-list

Creating Custom Service Definition (GUI)

Procedure

Step 1 Choose **Configuration > Services > mDNS**.

Step 2 In the **Service Definition** section, click **Add**.

Step 3 In the **Quick Setup: Service Definition** page that is displayed, enter a name and description for the service definition.

Step 4 Enter a service type and click **+** to add the service type.

Step 5 Click **Apply to Device**.

Creating Custom Service Definition

Service definition is a construct that provides an admin friendly name to one or more mDNS service types or A pointer (PTR) Resource Record Name.

By default, few built-in service definitions are already predefined and available for admin to use.

In addition to built-in service definitions, admin can also define custom service definitions.

You can execute the following command to view the list of all the service definitions (built-in and custom):

```
Device# show mdns-sd master-service-list
```

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition CUSTOM1`	Configures mDNS service definition. **Note** • All the created custom service definitions are added to the primary service list. • Primary service list comprises of a list of custom and built-in service definitions.
Step 4	**service-type** *string* **Example:** `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	Configures mDNS service type.
Step 5	**exit** **Example:** `Device(config-mdns-ser-def)# exit`	Returns to global configuration mode.

Creating Service List (GUI)

Procedure

Step 1 Choose **Configuration > Services > mDNS**.

Step 2 In the **Service List** section, click **Add**.

Step 3 In the **Quick Setup: Service List** page that is displayed, enter a name for the service list.

Step 4 From the **Direction** drop-down list, choose **IN** for inbound filtering or **OUT** for outbound filtering.

Step 5 From the **Available Services** drop-down list, choose a service type to match the service list.

Note To allow all services, choose the **all** option.

Step 6 Click **Add Services**.

Step 7 From the **Message Type** drop-down list, choose the message type to match from the following options:

- **any**—To allow all messages.
- **announcement**—To allow only service advertisements or announcements for the device.
- **query**—To allow only a query from the client for a service in the network.

Step 8 Click **Save** to add services.

Step 9 Click **Apply to Device**.

Creating Service List

mDNS service list is a collection of service definitions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**mdns-sd service-list** *service-list-name* {**IN** | **OUT**}
	Example:
	`Device(config)# mdns-sd service-list Basic-In IN`
	`Device(config)# mdns-sd service-list Basic-Out OUT`
		Configures mDNS service list.
		• **IN**: Provides inbound filtering.
		• **Out**: Provides outbound filtering.

Step 4	**match** *service-definition-name* **message-type** {**announcement** | **any** | **query**} **Example:** `Device(config-mdns-sl-in)# match CUSTOM1 message-type query`	Matches the service to the message type. Here, *service-definition-name* refers to the names of services, such as, airplay, airserver, airtunes, and so on. **Note** To add a service, the service name must be part of the primary service list. If the mDNS service list is set to IN, you get to view the following command: **match service-definition-name message-type {announcement | any | query}**. If the mDNS service list is set to Out, you get to view the following command: **match service-definition-name**.

	Command or Action	Purpose
		(OR)
Step 5	**match all message-type** {**announcement** | **any** | **query**} **Example:** `Device(config-mdns-sl-in)# match all message-type query`	Matches all services to the message type. **Note** To add a service, the service name must be part of the primary service list. If the mDNS service list is set to IN, you get to view the following command: **match all message-type {announcement | any | query}**. If the mDNS service list is set to OUT, you get to view the following command: **match all**. In case of IN or OUT filter, if any of the service contains the same or subset of the message type (query or announcement), the **match all** is not allowed unless the existing services are removed.
Step 6	**show mdns-sd service-list {direction | name }**	Displays inbound or outbound direction list of the configured service-list to classify matching service-types for service-policy. The list can be filtered by name or specific direction.
Step 7	**exit** **Example:** `Device(config-mdns-sl-in)# exit`	Returns to global configuration mode.

Creating Service Policy (GUI)

Procedure

Step 1 Choose **Configuration > Services > mDNS**.

Step 2 In the **Service Policy** section, click **Add**.

Step 3 In the **Quick Setup: Service Policy** page that is displayed, enter a name for the service policy.

Step 4 From the **Service List Input** drop-down list, choose one of the types.

Step 5 From the **Service List Output** drop-down list, choose one of the types.

Step 6 From the **Location** drop-down list, choose the location you want to associate with the service list.

Step 7 Click **Apply to Device**.

Creating Service Policy

mDNS service policy is used for service filtering while learning services or responding to queries.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged **EXEC** mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Enables mDNS service policy.
Step 4	**location** {**ap-location** | **ap-name** | **location-group** | **lss** | **regex** | **site-tag** | **ssid**} **Example:**	Filters mDNS service types based on location filter.

	Command or Action	Purpose
	`Device(config-mdns-ser-pol)# location lss`	**Note** • If location filter is not applied during service policy, the global location filter (default=**lss**) will be considered. • The location filter from the service policy takes precedence even if the global location filter is configured. • In Location Specific Services (LSS) based filtering, the mDNS gateway responds with the service instances learnt from the neighboring APs of the querying client AP. Other service instances for the rest of APs are filtered. • In Site tag based filtering, the mDNS gateway responds with the service instances that belong to the same site-tag as that of querying client. • The mDNS gateway responds back with wired services even if the location based filtering is configured.
Step 5	**service-list** *service-list-name* {**IN** | **OUT**} **Example:** `Device(config-mdns-ser-pol)# service-list VLAN100-list IN`	Configures various service-list names for IN and OUT directions. **Note** If an administrator decides to create or use a custom service policy, then the custom service policy must be configured with service-lists for both directions (IN and OUT); otherwise, the mDNS Gateway will not work (will not learn services if there is no IN service-list, or will not reply or announce services learned if there is no OUT service-list).
Step 6	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-mdns-ser-pol)# exit`	

Configuring a Local or Native Profile for an mDNS Policy

When an administrator configures local authentication and authorization and does not expect to get any mDNS policy from the AAA server, the administrator can configure a local or native profile to select a mDNS policy based on user, role, or device type. When this local or native profile is mapped to the wireless profile policy, mDNS service policy is applied on the mDNS packets that are processed on that WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**service-template** *template-name* **Example:** `Device(config)# service-template mdns`	Configures the service-template or identity policy.
Step 3	**mdns-service-policy** *mdns-policy-name* **Example:** `Device(config-service-template)# mdns-service-policy mdnsTV`	Configures the mDNS policy.
Step 4	**exit** **Example:** `Device(config-service-template)# exit`	Returns to global configuration mode.

Configuring an mDNS Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS**.

Step 2 In the **mDNS Flex Profile** section, click **Add**.
The **Add mDNS Flex Profile** window is displayed.

Step 3 In the **Profile Name** field, enter the flex mDNS profile name.

Step 4 In the **Service Cache Update Timer** field, specify the service cache update time. The default value is 1 minute. The valid range is from 1 to 100 minutes.

Step 5 In the **Statistics Update Timer** field, specify the statistics update timer. The default value is 1 minute. The valid range is from 1 to 100 minutes.

Step 6 In the **VLANs** field, specify the VLAN ID. You can enter multiple VLAN IDs separated by commas, or enter a range of VLAN IDs. Maximum number of VLANs allowed is 16.

Step 7 Click **Apply to Device**.

Configuring an mDNS Flex Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd flex-profile** *mdns-flex-profile-name* **Example:** `Device(config)# mdns-sd flex-profile mdns-flex-profile-name`	Enters the mDNS Flex Profile mode.
Step 3	**update-timer service-cache** *service-cache timer-value <1-100>* **Example:** `Device(config-mdns-flex-profile)# update-timer service-cache 60`	Configures the mDNS update service cache timer for the flex profile. The default value is 1 minute. Value range is between 1 minute and 100 minutes.
Step 4	**update-timer statistics** *statistics timer-value <1-100>* **Example:** `Device(config-mdns-flex-profile)# update-timer statistics 65`	Configures the mDNS update statistics timer for the flex profile. The default value is 1 minute. The valid range is from 1 to 100 minutes.
Step 5	**wired-vlan-range** *wired-vlan-range value* **Example:** `Device(config-mdns-flex-profile)# wired-vlan-range 10 - 20`	Configures the mDNS wired VLAN range for the flex profile. The default value is 1 minute. The valid range is from 1 minute to 100 minutes.

Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (GUI)

Procedure

Step 1 Choose **Configuration > Tags & Profiles > Flex**.

Step 2 Click **Add**.
The **Add Flex Profile** window is displayed.

Step 3 Under the **General** tab, from the **mDNS Flex Profile** drop-down list, choose a flex profile name from the list.

Step 4 Click **Apply to Device**.

Applying an mDNS Flex Profile to a Wireless Flex Connect Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *wireless-flex-profile-name* **Example:** `Device# wireless profile flex wireless-flex-profile-name`	Enters wireless flex profile configuration mode.
Step 3	**mdns-sd** *mdns-flex-profile* **Example:** `Device(config-wireless-flex-profile)# mdns-sd mdns-flex-profile-name`	Enables the mDNS features for all the APs in the profile

Enabling the mDNS Gateway on the VLAN Interface

This procedure configures the mDNS service policy for a specific VLAN. This allows the administrator to configure different settings to the mDNS packets on per VLAN interface basis and not on per WLAN basis.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-interface-number* **Example:** `Device(config)# interface vlan 200`	Configures a VLAN ID and enters interface configuration mode.

	Command or Action	Purpose
Step 3	**ip address** *ip-address subnet-mask* **Example:** `Device(config-if)# ip address 111.1.1.1 255.255.255.0`	Configures the IP address for the interface.
Step 4	**mdns-sd gateway** **Example:** `Device(config-if)# mdns-sd gateway`	Enables mDNS configuration on a VLAN interface.
Step 5	**service-policy** *service-policy-name* **Example:** `Device(config-if-mdns-sd)# service-policy test-mDNS-service-policy`	Configures the service policy. **Note** If specific *service-policy-name* is not defined, the VLAN will use the **default-mdns-service-policy** by default. By default, **default-mDNS-service-policy** gets created in the system and it will use **default-mDNS-service-list** configuration for filtering mDNS service announcement and queries.
Step 6	**end** **Example:** `Device(config-if-mdns-sd)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Location-Based Service Filtering

Prerequisite for Location-Based Service Filtering

You need to create the Service Definition and Service Policy. For more information, see Creating Custom Service Definition section and Creating Service Policy section.

Configuring mDNS Location-Based Filtering Using SSID

When a service policy is configured with the SSID as the location name, the response to the query will be the services that were learnt on that SSID.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures the service policy.
Step 3	**location ssid** **Example:** `Device(config-mdns-ser-pol)# location ssid`	Configures location-based filtering using SSID.
Step 4	**end** **Example:** `Device(config-mdns-ser-pol)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring mDNS Location-Based Filtering Using AP Name

When a service policy is configured with the AP name as the location, the response to the query will be the services that were learnt on that AP.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures the service policy.
Step 3	**location ap-name** **Example:** `Device(config-mdns-ser-pol)# location ap-name`	Configures location-based filtering using an AP name.
Step 4	**end** **Example:** `Device(config-mdns-ser-pol)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring mDNS Location-Based Filtering Using AP Location

When a service policy is configured with location as the AP-location, the response to the query will be the services that were learnt on all the APs using the same AP "location" name (not to be confused with "site-tag").

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures the service policy.
Step 3	**location ap-location** **Example:** `Device(config-mdns-ser-pol)# location ap-location`	Configures location-based filtering using the AP location.
Step 4	**end** **Example:** `Device(config-mdns-ser-pol)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring mDNS Location-Based Filtering Using Regular Expression

- When a service policy is configured with the location as a regular expression that matches the corresponding AP name, the response to the query will be the services that were learnt on a group of APs based on the AP name.
- When a service policy is configured with the location as a regular expression that matches the corresponding AP location, the response to the query will be the services that were learnt on a group of APs based on the AP location.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd service-policy** *service-policy-name* **Example:**	Configures the service policy.

	Command or Action	Purpose
	`Device(config)# mdns-sd service-policy mdns-policy1`	

Step 3	**location regex** {**ap-location** *regular-expression* | **ap-name** *regular-expression*}
	Example:
	`Device(config-mdns-ser-pol)# location regex ap-location dns_location`
	`Device(config-mdns-ser-pol)# location regex ap-name dns_name`
		Configures location-based filtering using regular expression.

Step 4	**end** **Example:** `Device(config-mdns-ser-pol)# end` **Note** To filter the services for which AP names have the specific keyword such as *AP-2FLR-SJC-123*, you can use the regex AP name as *AP-2FLR-* to match the services that are learnt from the set of access points.	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring mDNS Location-Based Filtering Using Location Group

Feature History for mDNS Location-Based Filtering Using Location Group (Microlocation)

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 164: Feature History for mDNS Location-Based Filtering Using Location Group (Microlocation)

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	mDNS Location-Based Filtering Using Location Group (Microlocation)	The controller is enhanced to support microlocation from wireless clients tagged with the location group (mDNS Group ID) tag. From Cisco IOS-XE 17.3 onwards, location grouping is done based on AP names. From Cisco IOS-XE 17.9 onwards, location grouping is extended to AP location.

Information About mDNS Location-Based Filtering Using Location Group (Microlocation)

In the context of Apple Bonjour, Microlocation refers to the smaller subset of a wireless location. This is also referred to as mDNS AP Group or Location Group.

To create an mDNS AP location group, perform the following procedure:

1. Define multiple rules with priority in the wireless rule-based mDNS application.

Note The rules have AP microlocation grouping as AP name or AP location.

2. Match the highest priority rule-based on the configured regular expression with AP name and AP location-based grouping.
3. Map an AP to a location group (mDNS Group ID).

Note When you delete or modify a rule, the corresponding APs are revalidated (using the **capwap restart** command) to apply the updated configuration.

AP Microlocation Support Based on AP Location

From Cisco IOS-XE 17.3 onwards, AP location is configured using the **ap name** *name* **location** *location* command.

From Cisco IOS-XE 17.9 onwards, AP location is leveraged to group APs belonging to a location to form a location group.

By default, AP microlocation, based on either AP name or AP location, is disabled.

Use Cases for mDNS Location-Based Filtering Using Location Group (Microlocation)

- Restricts services across departments.
- Shares files across building or sites.
- Teachers or students, doctors or patients, employees or groups need service visibility in contained environment without intervening with IT to change to L2 or L3 networks.

Prerequisites for mDNS Location-Based Filtering Using Location Group (Microlocation)

You must have configured the mDNS rule. By default, the AP name-based microlocation grouping is used.

Enabling Location Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures mDNS service policy.

Step 3	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config-mdns-ser-pol)# service-list VLAN100-list in`
	`Device(config-mdns-ser-pol)# service-list VLAN300-list out`
		Configures service lists for IN and OUT directions.

Step 4	**location location-group** **Example:** `Device(config-mdns-ser-pol)# location location-group`	Configures location-based filtering using location group.
Step 5	**end** **Example:** `Device(config-mdns-ser-pol)# end`	Returns to privileged EXEC mode.

Adding APs to a Location Group (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless rule application mdns** **Example:** `Device(config)# wireless rule application mdns`	Configures wireless rule-based MDNS application.
Step 3	**rule-priority** *rule_priority* **rule-name** *rule_name* **Example:** `Device(config-app-rule)# rule-priority 2011 rule-name R2011`	Configures rule priority. Here, • *rule_priority*: The valid range is from 0 to 4096. **Note** 0 is the lower priority number and 4096 is the higher priority number.

	Command or Action	Purpose
		• *rule_name*: The rule name can be between 1 to 32 characters. **Note** When you configure the rule priority, you will be prompted as follows: `Changing regex string or other rule configuration may cause associated APs to rejoin` When you see this prompt, enter **Y** to continue with the configuration.
Step 4	**regex** *regular_expression_string* **Example:** `Device(config-rule-params)# regex AP_Name`	Configures rule-based on AP name or AP location to match the regular expression.
Step 5	**action-type grouping** **Example:** `Device(config-rule-params)# action-type grouping`	Groups APs based on the filter string.
Step 6	**group-id** *location_group_identifier* **Example:** `Device(config-rule-action-mdns)# group-id 44`	Configures the mDNS location group identifier. Valid range for *location_group_identifier* is 1 to 4096.
Step 7	**group-method ap location** **Example:** `Device(config-rule-action-mdns)# group-method ap location`	Configures AP location-based grouping. **Note** If you consider **group-method** as **ap location**, the regex captures the *AP_LOC_NAME*. By default, the **group-method** is configured with *AP_NAME*.
Step 8	**group-name** *location_group_name* **Example:** `Device(config-rule-action-mdns)# group-name G2011`	Configures mDNS location group name.
Step 9	**end** **Example:** `Device(config-rule-action-mdns)# end`	Returns to privileged EXEC mode.

Verifying AP Location

To verify the mDNS location Group ID associated with an AP, use the following command:

```
Device# show ap config general | sec MDNS | AP Name
Cisco AP Name   : AP2800
MDNS Group Id                                   : 101
MDNS Rule Name                                  : R101
MDNS Group Method                               : AP Location
```

To verify all the APs associated with the configured mDNS rule name, use the following command:

```
Device# show wireless associated-ap mdns-rule-name R1
AP MAC              AP Name
-----------------------------------------------------------------
0cd0.f894.a840      AP0CD0.F894.083C
4001.7a03.8560      APA023.9F66.4F96
--------------------
```

To verify all the APs associated with the configured mDNS location group ID, use the following command:

```
Device# show wireless associated-ap mdns-group-id 1

AP MAC              AP Name
-----------------------------------------------------------------
0cd0.f894.a840      AP0CD0.F894.083C
4001.7a03.8560      APA023.9F66.4F96
--------------------
```

To verify the mDNS group method detail for each AP, use the following command:

```
Device# show ap config general | inc MDNS|AP Name|Location
Cisco AP Name   : AP-1
MDNS Group Id                                   : 100
MDNS Rule Name                                  : R100
MDNS Group Method                               : AP Location
```

To verify the mDNS group method detail for each rule, use the following command:

```
Device# show wireless rule application mdns
Rule Name          : R100
Rule Priority      : 100
Regular Expression : AP0
Action Type        : MDNS Grouping
  MDNS Group ID    : 100
MDNS Group Name  : G100
MDNS Group Method: AP Location
```

Nearest mDNS-Based Wired Service Filtering

Feature History for Nearest mDNS-Based Wired Service Filtering

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 165: Feature History for Nearest mDNS-Based Wired Service Filtering

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	Nearest mDNS-Based Wired Service Filtering	This feature supports the following functionalities: • Nearest mDNS based wired service filtering. (Supported in Central switched Local mode.) • Custom wired service policy support for FlexConnect mode. • VLAN and MAC based wired service filtering. (Supported in Central switched Local mode.)

Information About Nearest mDNS-Based Wired Service Filtering

Prior to Cisco IOS XE 17.8.1 release, the wireless clients discover the following:

- All wired services from mDNS-AP.
- Service providers on VLANs visible to the controller.

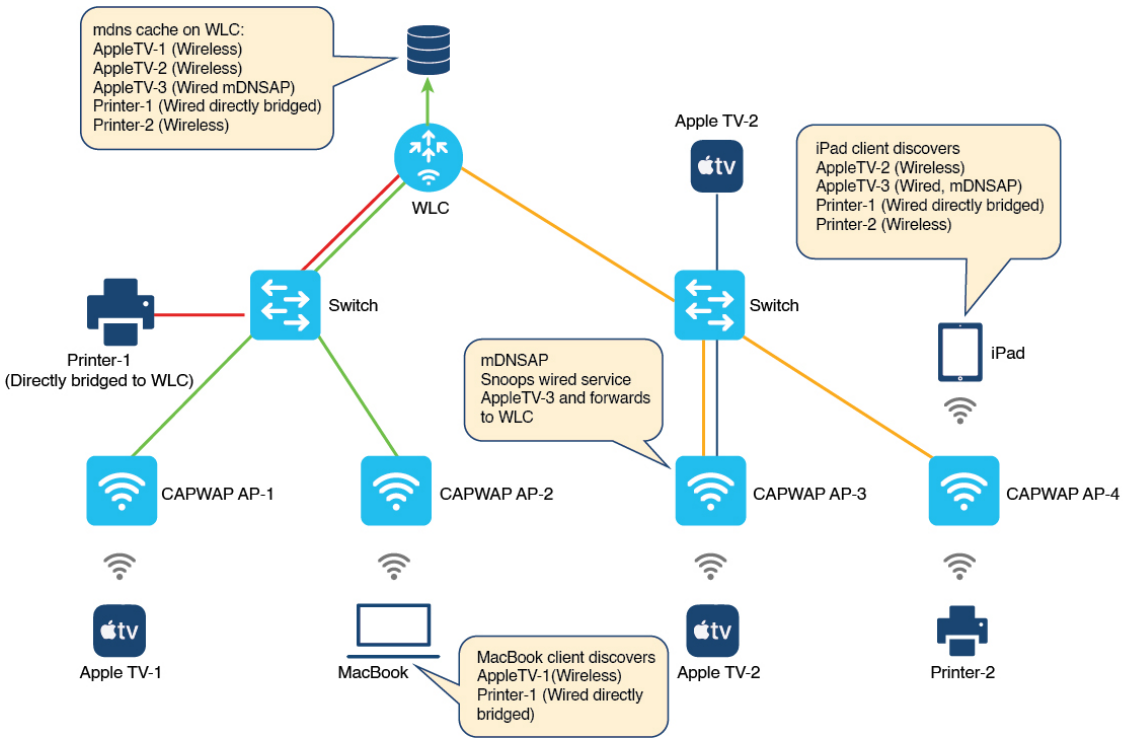
Note The current filtering is supported only for wireless services.

From Cisco IOS XE 17.8.1 onwards, the wireless clients are enhanced to support filter-based on the nearest wired service provider.

Note The controller classifies the wired services as the nearest wired services once the LSS is enabled. The mDNS-AP forwards or advertises the nearest wired services.

The following figure illustrates the nearest wired service provider and discovery:

Figure 83: Nearest Wired Service Provider and Discovery



As per the figure, the controller is associated with the following four APs:

- CAPWAP AP-1
- CAPWAP AP-2
- CAPWAP AP-3
- CAPWAP AP-4

The client connected to CAPWAP AP-1 is wireless and advertises the service Apple TV-1.

Similarly, the client connected to CAPWAP AP-2 is wireless and advertises the service MacBook query client.

The CAPWAP AP-3 is enabled as an mDNS-AP. This AP then discovers the wired services on VLANs and forwards them to the controller. In this case, the client advertising the service AppleTV-3 is a wired service. The client is then discovered by CAPWAP AP-3 and forwarded to the controller. You will also view another client connected to CAPWAP AP-3 that is wireless and advertises the service AppleTV-2.

The client connected to CAPWAP AP-4 is wireless and advertises the service Printer-2 and iPad query client.

Also, a client is connected directly to the controller, which advertises the Printer-1.

The controller covers cache populated from both wireless and wired service providers.

The controller populates the following cache:

- AppleTV-1 (Wireless service from CAPWAP AP-1)
- AppleTV-2 (Wireless service from CAPWAP AP-3)
- AppleTV-3 (Wired service from mDNS-AP enabled AP-3)

- Printer-1 (Wired service from directly bridged service provider)
- Printer-2 (Wireless service from AP-4)

When LSS is enabled, AP-1 and AP-2 discover each other as LSS neighbors. Similarly, AP-3 and AP-4 discover each other as LSS neighbors.

MacBook discovers the following services:

- AppleTV-1 (Wireless service from AP-1)
- Printer-1 (Wired service from the directly bridged service provider)

Note MacBook does not discover the wired service AppleTV-3 (forwarded by mDNS-AP AP-3). The AP-2 does not see AP-3 as the LSS neighbor. Thus, the controller does not classify the wired service AppleTV-3 as nearby.

iPad discovers the following services:

- AppleTV-2 (Wireless service from AP-3)
- AppleTV-3 (Wired service from mDNS-AP enabled AP-3)
- Printer-1 (Wired service from directly bridged service provider)
- Printer-2 (Wireless service from AP-4)

Note iPad discovers the wired service AppleTV-3 (forwarded by mDNS-AP AP-3). The AP-4 sees AP-3 as the LSS neighbor. Thus, the controller classifies the wired service AppleTV-3 as nearby.

Note This feature supports only the wired services advertised by mDNS-AP in centrally switched local mode.

Information About Custom Wired Service Policy Support for FlexConnect Mode

From Cisco IOS XE 17.8.1 release onwards, the custom service policy for wired services is supported in a Flex profile. Here, the service policy refers to the mDNS service policy.

Information About VLAN and MAC Based Wired Service Filtering

Prior to Cisco IOS XE 17.8.1 release, service filtering was based on service types, location type, and location filter. These filters are applicable for wireless services. However, they are not supported for wired services.

From Cisco IOS XE 17.8.1 release onwards, the VLAN and MAC based filtering is supported for wired services.

Note

- In case of wired services, the VLAN and MAC based filtering is applicable for OUT direction filter advertised by mDNS-AP and directly bridged wired services.
- The VLAN and MAC based filtering is applicable for centrally switched local mode.

Prerequisite for Nearest mDNS-Based Wired Service Filtering

- Enable the mDNS gateway on the controller.

Use Cases

The following are the use cases:

- Nearest mDNS-Based Wired Service Filtering.
- Custom Wired Service Policy Support for FlexConnect Mode.
- VLAN and MAC Based Wired Service Filtering.

While migrating from AireOS wireless controllers to the Cisco Catalyst 9800 Series Wireless Controllers, the following limitations occur:

- The wireless clients discover all the wired services and not just the nearby service from the wired service provider when central switched local mode and LSS in enabled.

  The wired services belong to the forwarded mDNS-AP and directly bridged ones.

- There is no provision to apply the custom service policy for wired services when locally switched FlexConnect mode is enabled.

  The mDNS flex profile must have the custom wired service policy as well.

- There is no provision to filter based on the VLAN and MAC address for wired services in centrally switched local mode.

Configuring Wired Service Policy Support in Flex Profile

Creating Service List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-list** *service-list-name* **IN** **Example:** `Device(config)# mdns-sd service-list srvc_list_in IN`	Configures mDNS service list for inbound filtering.

Step 4	**match** *service-definition-name*
	Example:
	`Device(config)# match airplay`
	Example:
	`Device(config)# match printer_ipp`
		Matches the service to the service definition name. Here, *service-definition-name* refers to the names of services, such as, airplay, airserver, airtunes, and so on.
		Note To add a service, the service name must be part of the primary service list.
		The same set of service list will be used for both IN and OUT filters.

Step 5	**mdns-sd service-list** *service-list-name* **OUT** **Example:** `Device(config)# mdns-sd service-list srvc_lst_out OUT`	Configures mDNS service list for outbound filtering.
Step 6	**match** *service-definition-name* **Example:** `Device(config-mdns-sl-out)# match airplay`	Matches the service to the service definition name. Here, *service-definition-name* refers to the names of services, such as, airplay, airserver, airtunes, and so on. **Note** To add a service, the service name must be part of the primary service list. The same set of service list will be used for both IN and OUT filters.
Step 7	**exit** **Example:** `Device(config-mdns-sl-out)# exit`	Exits mDNS service list configuration mode.

Creating Service Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd** *service-policy* **service-policy-name** **Example:** `Device(config)# mdns-sd service-policy custom_wired_policy`	Configures mDNS service policy.

Step 4	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config-mdns-ser-pol)# service-list srvc_list_in IN`
	`Device(config-mdns-ser-pol)# service-list srvc_list_out OUT`
		Configures service lists for IN and OUT directions.

Step 5	**location lss** **Example:** `Device(config-mdns-ser-pol)# location lss`	Enables Location Specific Services (LSS) for the mDNS service.
Step 6	**exit** **Example:** `Device(config-mdns-ser-pol)# exit`	Exits mDNS service policy configuration mode.

Configuring an mDNS Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **mDNS**.

Step 2 In the **mDNS Flex Profile** section, click **Add**.

Step 3 In the **Add mDNS Flex Profile** window that is displayed, enter the Flex mDNS profile name in the **Profile Name** field.

Step 4 In the **Service Cache Update Timer** field, specify the service cache update time. The value range is between 1 and 100 minutes.

Step 5 In the **Statistics Update Timer** field, specify the statistics update timer. The value range is between 1 and 100 minutes.

Step 6 In the **VLANs** field, specify the VLAN ID. You can enter multiple VLAN IDs separated by commas or enter a range of VLAN IDs. Maximum number of VLANs allowed is 16.

Step 7 Enter or select a **Wired Service Policy** from the drop-down list to associate a Wired filter to mDNS Flex-Profile. In addition to filtering mDNS service queries based on the static default service list, wired filter will support filtering based on custom service lists.

The new wired service-policy will be added to flex-profile construct to support the custom wired service-policy. The AP will apply this configuration for wired services and the respective IN and OUT filters will be used for advertisements and queries only if the custom wired service-policy is configured in mDNS flex-profile.

In case a custom service-policy is removed from the mDNS flex-profile, the AP will remove the custom service-policy and apply the default service-policy for wired services. This feature is supported only in locally switched FlexConnect mode.

Step 8 Click **Apply to Device**.

Configuring an mDNS Flex Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd flex-profile** *mdns-flex-profile-name* **Example:** `Device(config)# mdns-sd flex-profile custom_flex_profile`	Configures an mDNS Flex profile.
Step 4	**update-timer service-cache** *timer-value <1-100>* **Example:** `Device(config-mdns-flex-prof)# update-timer service-cache 15`	Configures the mDNS update service cache timer for the flex profile. The default value is 1 minute. Value range is between 1 minute and 100 minutes.
Step 5	**update-timer statistics** *statistics timer-value <1-100>* **Example:** `Device(config-mdns-flex-prof)# update-timer statistics 10`	Configures the mDNS update statistics timer for the flex profile. The default value is 1 minute. The valid range is from 1 to 100 minutes.

	Command or Action	Purpose
Step 6	**wired-vlan-range** *wired-vlan-range value* **Example:** `Device(config-mdns-flex-prof)# wired-vlan-range 30`	Configures the mDNS wired VLAN range for the flex profile. The default value is 1 minute. The valid range is from 1 minute to 100 minutes.
Step 7	**wired-service-policy** *service-policy-name* **Example:** `Device(config-mdns-flex-prof)# wired-service-policy custom_wired_policy`	Associates the wired service policy with mDNS flex profile. **Note** Here, *service-policy-name* refers to the mDNS service policy created earlier. For more information, refer to Creating Service Policy (CLI).
Step 8	**end** **Example:** `Device(config-mdns-flex-prof)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring VLAN and MAC Based Wired Service Filtering (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd wired-filter** *wired-filter-name* **Example:** `Device(config)# mdns-sd wired-filter WIRED_FILTER_APPLE_TV`	Configures an mDNS wired filter.
Step 4	**match mac** *service-provider-mac-address1* **Example:** `Device(config-mdns-wired-filter)# match mac a886.ddb2.05e9`	Matches the wired filter with the MAC address of the wired service.
Step 5	**match vlan** *range* **Example:** `Device(config-mdns-wired-filter)# match vlan 100`	Matches the wired filter with the VLAN of the wired service.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-mdns-wired-filter)# exit`	Exits mDNS gateway configuration mode.
Step 7	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 8	**mdns-sd service-list** *service-list-name* **IN** **Example:** `Device(config)# mdns-sd service-list srvc_lst_in IN`	Configures mDNS service list for inbound filtering.
Step 9	**match** *service-definition-name* **Example:** `Device(config)# match airplay`	Matches the service to the names of the services. Here, *service-definition-name* refers to the names of services, such as, airplay, airserver, airtunes, and so on.
Step 10	**mdns-sd service-list** *service-list-name* **OUT** **Example:** `Device(config)# mdns-sd service-list srvc_lst_out OUT`	Configures mDNS service list for outbound filtering.
Step 11	**match apple-tv wired-filter** *wired-filter-name* **Example:** `Device(config-mdns-sl-out)# match apple-tv wired-filter WIRED_FILTER_APPLE_TV`	Matches the Apple TV related wired filter.
Step 12	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy custom_policy`	Enables mDNS service policy.

Step 13	**service-list** *service-list-name* {**IN** | **OUT**}
	Example:
	`Device(config-mdns-ser-pol)# service-list srvc_lst_in IN`
	`Device(config-mdns-ser-pol)# service-list srvc_lst_in OUT`
		Configures various service-list names for IN and OUT directions.
		Note If an administrator decides to create or use a custom service policy, then the custom service policy must be configured with service-lists for both directions (IN and OUT); otherwise, the mDNS Gateway will not work (will not learn services if there is no IN service-list, or will not reply or announce services learned if there is no OUT service-list).

	Command or Action	Purpose
Step 14	**location ap-group** **Example:** `Device(config-mdns-ser-pol)# location ap-group`	Configures AP location based filtering.
Step 15	**end** **Example:** `Device(config-mdns-ser-pol)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying mDNS-Based Wired Service Filtering

To view the wired service list IN and OUT details, use the following command:

```
Device# show mdns status

Global mDNS gateway:Enabled

vap_id      ssid mdns_mode
     0  myFisaiC    Bridge
     1 rguestcpC    Bridge
     2   RK-FLEX    Bridge
     3   RK-MDNS   Gateway
     4 GUHOAsaiC    Bridge
     5         -    Bridge
     6         -    Bridge
     7         -    Bridge
     8         -    Bridge
     9         -    Bridge
    10         -    Bridge
    11         -    Bridge
    12         -    Bridge
    13         -    Bridge
    14         -    Bridge
    15         -    Bridge
Active query interval:30
vap              service_list_in              service_list_out location
  0 default-mdns-service-list_IN default-mdns-service-list_OUT        0
  1 default-mdns-service-list_IN default-mdns-service-list_OUT        0
  2 default-mdns-service-list_IN default-mdns-service-list_OUT        0
  3 default-mdns-service-list_IN default-mdns-service-list_OUT        0
  4 default-mdns-service-list_IN default-mdns-service-list_OUT        0
Wired vlan configuration:
mdns stats timer: 1
mdns cache timer: 1
AP Sync VLAN: 1
Wired service list IN: RK-IN_IN
Wired service list OUT: RK-OUT_OUT
```

Note This command must be executed on the Flex AP. Also, this applies to the custom wired service policy support in FlexConnect mode.

To verify the VLAN and MAC based wired service filtering, use the following command:

```
Device# show running-config mdns-sd wired-filter
mdns-sd wired-filter WIRED_FILTER_APPLE_TV
match mac a886.ddb2.05e9
match vlan 100
!
```

To verify the wired service policy support in Flex Profile, use the following command:

```
Device# show running-config mdns-sd flex-profile
mdns-sd flex-profile custom_flex_profile
update-timer service-cache 15
update-timer statistics 10
wired-vlan-range 30
wired-service-policy custom_wired_policy
!
```

To verify whether LSS is configured or not, use the following command:

```
Device# show running-config mdns-sd service-policy
mdns-sd service-policy custom_policy
service-list srvc_lst_in IN
service-list srvc_lst_out OUT
location lss
!
mdns-sd service-list srvc_lst_in IN
match apple-tv
!

mdns-sd service-list srvc_lst_out OUT
match apple-tv wired-filter WIRED_FILTER_APPLE_TV
!
```

Configuring mDNS AP

In most of the deployments, the services may be available in VLANs that the APs can hear in the wired side (allowed in the switchport where the AP is directly connected: its own VLAN, or even more VLANs if switchport is a trunk).

The following procedure shows how to configure mDNS AP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Configures the mDNS gateway.
Step 3	**ap name** *ap-name* **mdns-ap enable vlan** *vlan-id* **Example:**	Enables mDNS on the AP, and configures a VLAN for the mDNS AP.

	Command or Action	Purpose
	`Device# ap name ap1 mdns-ap enable vlan 22`	
Step 4	**ap name** *ap-name* **mdns-ap vlan add** *vlan-id* **Example:** `Device# ap name ap1 mdns-ap vlan add 200`	Adds a VLAN to the mDNS AP. *vlan-id* ranges from 1 to 4096.
Step 5	**ap name** *ap-name* **mdns-ap vlan del** *vlan-id* **Example:** `Device# ap name ap1 mdns-ap vlan del 2`	Deletes a VLAN from the mDNS AP.
Step 6	**ap name** *ap-name* **mdns-ap disable** **Example:** `Device# ap name ap1 mdns-ap disable`	(Optional) Disables the mDNS AP.
Step 7	**end** **Example:** `Device# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. **Note** You can configure a maximum of 10 VLANs per AP.

Enabling mDNS Gateway on the RLAN Interface

By configuring the mDNS gateway mode on the RLAN interface, you can configure the mDNS service policy for a specific RLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap remote-lan profile-name** *remote-lan-profile-name rlan-id* **Example:** `Device(config)# ap remote-lan profile-name rlan_test_1 1`	Configures a remote LAN profile. • *remote-lan-profile*: Remote LAN profile name. Range is from 1 to 32 alphanumeric characters. • *rlan-id*: Remote LAN identifier. Range is from 1 to 128.

	Command or Action	Purpose
		Note You can create a maximum of 128 RLANs. Also, you cannot use the *rlan-id* of an existing RLAN while creating another RLAN.
Step 3	**mdns-sd-interface {gateway | drop}** **Example:** mdns-sd-interface `Device(config-remote-lan)# mdns-sd-interface gateway`	Enables mDNS configuration on an RLAN interface.
Step 4	**no shutdown** **Example:** `Device(config-remote-lan)# no shutdown`	Restarts the RLAN profile.
Step 5	**exit** **Example:** `Device(config-remote-lan)# exit`	Exits remote LAN configuration mode.
Step 6	**ap remote-lan-policy policy-name** *profile name* **Example:** `Device(config)# ap remote-lan-policy policy-name rlan_named_pp1`	Configures the RLAN policy profile and enters wireless policy configuration mode.
Step 7	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config-remote-lan-policy)# mdns-sd service-policy mdnsTV6`	Enables an mDNS service policy.
Step 8	**central switching** **Example:** `Device(config-remote-lan-policy)# central switching`	Configures the RLAN for central switching.
Step 9	**central dhcp** **Example:** `Device(config-remote-lan-policy)# central dhcp`	Configures the central DHCP for centrally switched clients.
Step 10	**vlan** *vlan-name* **Example:** `Device(config-remote-lan-policy)# vlan 141`	Assigns the profile policy to a VLAN.

	Command or Action	Purpose
Step 11	**no shutdown** **Example:** `Device(config-remote-lan-policy)# no shutdown`	Restarts the RLAN profile.
Step 12	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy rlan_pt_1`	Configures a policy tag.

Step 13	**remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*
	Example:
	`Device(config-policy-tag)# remote-lan rlan_test_1 policy rlan_named_pp1 port-id 1`
	`Device(config-policy-tag)# remote-lan rlan_test_1 policy rlan_named_pp1 port-id 2`
	`Device(config-policy-tag)# remote-lan rlan_test_1 policy rlan_named_pp1 port-id 3`
	`Device(config-policy-tag)# remote-lan rlan_test_1 policy rlan_named_pp1 port-id 4`
		Maps the RLAN policy profile to the RLAN profile.
		• *remote-lan-profile-name*: Name of the RLAN profile.
		• *rlan-policy-profile-name*: Name of the policy profile.
		• *port-id*: LAN port number on the access point. Range is from 1 to 4.

Step 14	**exit** **Example:** `Device(config-policy-tag)# exit`	Returns to global configuration mode.
Step 15	**ap** *mac-address* **Example:** `Device (config)# ap 0042.5AB6.0EF0`	Configures the AP and enters the AP tag configuration mode. **Note** Use the Ethernet MAC address.
Step 16	**policy-tag** *policy-tag-name* **Example:** `Device (config-ap-tag)# policy-tag rlan_pt_1`	Maps a policy tag to the AP.
Step 17	**end** **Example:** `Device(config-guest-lan)# end`	Returns to privileged EXEC mode.

Enabling mDNS Gateway on Guest LAN Interface

By configuring the mDNS gateway mode on a Guest LAN interface, you can configure the mDNS service policy for a specific Guest LAN interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**guest-lan profile-name** *guest_lan_profile_name num* **wired-vlan** *wired_vlan_num* **Example:** `Device(config)# guest-lan profile-name open 1 wired-vlan 666`	Configures guest LAN profile with a wired VLAN. **Note** Configures the wired VLAN only for the Guest Foreign controller. • *num*: Guest LAN identifier. The valid range is from 1 to 5. • *wired_vlan_num*: Wired VLAN number. The valid range is from 1 to 4094.
Step 3	**guest-lan profile-name** *guest_lan_profile_name num* **Example:** `Device(config)# guest-lan profile-name open 1`	Configures the guest LAN profile without a VLAN for the Guest Anchor controller.
Step 4	**mdns-sd-interface {gateway | drop}** **Example:** `Device(config-guest-lan)# mdns-sd gateway`	Configures the mDNS gateway for a Guest LAN. **Note** You need to enable mDNS gateway globally for the Guest LAN to work.
Step 5	**end** **Example:** `Device(config-guest-lan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Associating mDNS Service Policy with Wireless Profile Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the **policy profile** name.

Step 3 In the **Advanced** tab, choose the mDNS service policy from the **mDNS Service Policy** drop-down list.

Step 4 Click **Update & Apply to Device**.

Associating mDNS Service Policy with Wireless Profile Policy

Note You must globally configure the mDNS service policy before associating it with the wireless profile policy.

A default mDNS service policy is already attached once the wireless profile policy is created. You can use the following commands to override the default mDNS service policy with any of your service policy:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures wireless profile policy. Here, *profile-policy* refers to the name of the WLAN policy profile.
Step 3	**mdns-sd service-policy** *custom-mdns-service-policy* **Example:** `Device(config-wireless-policy)# mdns-sd service-policy custom-mdns-service-policy`	Associates an mDNS service policy with the wireless profile policy. The default mDNS service policy name is **default-mdns-service-policy**.

	Command or Action	Purpose
		Note

	Command or Action	Purpose
		The **default-mdns-profile-policy** uses **default-mdns-service-list** configuration for filtering mDNS service announcement and queries. In wireless network, the mDNS packets are consumed by the mDNS gateway and clients or device is deprived of learning this service. To share the service with the device and provide ease of configuration to the administrator, a list of few standard service types are shared by default on the wireless network. The list of such standard service types is termed as default service policy that comprises a set of service types. The table covers a sample service list in the default service policy.

Table 166: Default Name and mDNS Service Type

Default Name	mDNS Service Type
Apple TV	_airplay._tcp.local _raop._tcp.local
Apple HomeSharing	_home-sharing._tcp.local
Printer-IPPS	_ipps._tcp.local
Apple-airprint	_ipp._tcp.local _universal._sub._ipp._tcp.local
Google-chromecast	_googlecast._tcp.local _googlerpc._tcp.local _googlezone._tcp.local
Apple-remote-login	_sftp-ssh._tcp.local _ssh._tcp.local
Apple-screen-share	_rfb._tcp.local
Google-expeditions	_googexpeditions._tcp.local

	Command or Action	Purpose
		<table><tr><th>Default Name</th><th>mDNS Service Type</th></tr><tr><td>Multifunction-printer</td><td>_fax-ipp._tcp.local _ipp._tcp.local _scanner._tcp.local</td></tr><tr><td>Apple-windows-fileshare</td><td>_smb._tcp.local</td></tr></table> **Note** • Location would be disabled on mDNS default service policy. • You cannot change the contents of the mDNS default service policy. However, you can create separate mDNS service policies and associate them under the wireless policy profile.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.

Enabling or Disabling mDNS Gateway for WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click on the WLAN.

Step 3 In the **Advanced** tab, choose the mode in **mDNS Mode** drop-down list.

Step 4 Click **Update & Apply to Device**.

Enabling or Disabling mDNS Gateway for WLAN

Note Bridging is the default behaviour. This means that the mDNS packets are always bridged.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan test 24 ssid1`	Specifies the WLAN name and ID. • *profile-name* is the WLAN name which can contain 32 alphanumeric characters • *wlan-id* is the wireless LAN identifier. The valid range is from 1 to 4096. • *ssid-name* is the SSID which can contain 32 alphanumeric characters. **Note** Global configuration must be in place for mDNS gateway to work.

Step 3	**mdns-sd-interface** {**gateway** | **drop**}
	Example:
	`Device(config-wlan)# mdns-sd gateway`
	`Device(config-wlan)# mdns-sd drop`
		Enables or disables mDNS gateway and bridge functions on WLAN.

Step 4	**exit** **Example:** `Device(config-wlan)# exit`	Returns to global configuration mode.
Step 5	**show wlan name** *wlan-name* | **show wlan all** **Example:** `Device# show wlan name test | show wlan all`	Verifies the status of mDNS on WLAN.
Step 6	**show wireless profile policy** **Example:** `Device# show wireless profile policy`	Verifies the service policy configured in WLAN.

mDNS Gateway with Guest Anchor Support and mDNS Bridging

When mDNS Gateway is enabled on both Anchor and Foreign controller, the mDNS gateway functionality is supported in guest anchor deployment where clients on guest LAN or WLAN with guest anchor enabled will be responded with any services or cache from export foreign controller itself. All advertisements received on Guest LAN or WLAN on export foreign are learnt on the export foreign itself. All queries received on guest LAN or WLAN are responded by the export foreign itself.

When mDNS Gateway is enabled on Anchor and Disabled on Foreign controller [Bridging Mode], the mDNS gateway functionality is supported in guest anchor deployment where clients on guest LAN or WLAN with guest anchor enabled will be responded with any services or cache from export Anchor even though the clients are connected on Foreign. All advertisements received on guest LAN or WLAN on export foreign is forwarded to Anchor and the cache is stored on the Anchor itself. All queries received on guest LAN or WLAN are responded by the export Anchor itself.

Note

- You must configure the guest-LAN to a wireless profile policy which is configured with the required mDNS service-policy.
- To configure non guest LAN mDNS gateway, see the mDNS Gateway chapter.

Configuring mDNS Gateway on Guest Anchor

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**guest-lan profile-name** *guest-lan-profile-name guest-lan-id* **Example:** `Device(config)# guest-lan profile-name g-lanpro 2`	Configures the guest LAN profile with a wired VLAN.
Step 3	**mdns-sd gateway** **Example:** `Device(config-guest-lan)# mdns-sd gateway`	Enables mDNS gateway on the guest LAN.

Configuring mDNS Gateway on Guest Foreign (Guest LAN)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**guest-lan profile-name** *guest-lan-profile-name guest-lan-id* **wired-vlan** *vlan-id* **Example:** `Device(config)# guest-lan profile-name g-lanpro 2 wired-vlan 230`	Configures guest LAN profile with a wired VLAN. **Note** Configure the wired VLAN only for the Guest Foreign controller.
Step 3	**mdns-sd gateway** **Example:** `Device(config-guest-lan)# mdns-sd gateway`	Enables mDNS gateway on the guest LAN.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.

Configuring mDNS Gateway on Guest Anchor

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**guest-wlan profile-name** *guest-lan-profile-name guest-wlan-id* **Example:** `Device(config)# guest-wlan profile-name g-lanpro 2`	Configures the guest WLAN profile with a wired VLAN.
Step 3	**mdns-sd gateway** **Example:** `Device(config-guest-wlan)# mdns-sd gateway`	Enables mDNS gateway on the guest WLAN.

Configuring mDNS Gateway on Guest Foreign (Guest WLAN)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**guest-wlan profile-name** *guest-lan-profile-name guest-wlan-id* **wired-vlan** *vlan-id* **Example:** `Device(config)# guest-wlan profile-name g-lanpro 2 wired-vlan 230`	Configures guest WLAN profile with a wired VLAN. **Note** Configure the wired VLAN only for the Guest Foreign controller.
Step 3	**mdns-sd gateway** **Example:** `Device(config-guest-wlan)# mdns-sd gateway`	Enables mDNS gateway on the guest WLAN.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.

Verifying mDNS Gateway Configurations

To verify the mDNS summary, use the following command:

```
Device# show mdns-sd summary
mDNS Gateway: Enabled
Active Query: Enabled
  Periodicity (in minutes): 30
Transport Type: IPv4
```

To verify the mDNS cache, use the following command:

```
Device# show mdns-sd cache
------------------------------------------------------------ PTR Records
---------------------------------------
RECORD-NAME                     TTL      WLAN   CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
_airplay._tcp.local             4500     30     07c5.a4f2.dc01   CUST1._airplay._tcp.local

_ipp._tcp.local                 4500     30     04c5.a4f2.dc01   CUST3._ipp._tcp.local2

_ipp._tcp.local                 4500     15     04c5.a4f2.dc01   CUST3._ipp._tcp.local4
```

```
_ipp._tcp.local                 4500     10     04c5.a4f2.dc01   CUST3._ipp._tcp.local6

_veer_custom._tcp.local         4500     10     05c5.a4f2.dc01
CUST2._veer_custom._tcp.local8
```

To verify the mDNS cache from wired service provider, use the following command:

```
Device# show mdns-sd cache wired
------------------------------------------------------------ PTR Records
---------------------------------------
RECORD-NAME                               TTL      VLAN      CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
_airplay._tcp.local                         4500     16        0866.98ec.97af
wiredapple._airplay._tcp.local
_raop._tcp.local                            4500     16        0866.98ec.97af
086698EC97AF@wiredapple._raop._tcp.local

------------------------------------------------------------ SRV Records
---------------------------------------
RECORD-NAME                               TTL      VLAN      CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
wiredapple._airplay._tcp.local              4500     16        0866.98ec.97af   0 0 7000
wiredapple.local
086698EC97AF@wiredapple._raop._tcp.local    4500     16        0866.98ec.97af   0 0 7000
wiredapple.local

------------------------------------------------------------ A/AAAA Records
---------------------------------------
RECORD-NAME                               TTL      VLAN      CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
wiredapple.local                            4500     16        0866.98ec.97af
2001:8:16:16:e5:c446:3218:7437

------------------------------------------------------------ TXT Records
---------------------------------------
RECORD-NAME                               TTL      VLAN      CLIENT-MAC       RR-RECORD-DATA

-------------------------------------------------------------------------------------------------------------
wiredapple._airplay._tcp.local              4500     16        0866.98ec.97af
[343]'acl=0''deviceid=08:66:98:EC:97:AF''features=
086698EC97AF@wiredapple._raop._tcp.local    4500     16        0866.98ec.97af
[193]'cn=0,1,2,3''da=true''et=0,3,5''ft=0x5A7FFFF7
```

To verify the mdns-sd type PTR, use the following command:

```
Device# show mdns-sd cache type {PTR | SRV | A-AAA | TXT}
RECORD-NAME                                    TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------
_custom1._tcp.local                            4500     2         c869.cda8.77d6
service_t1._custom1._tcp.local
_custom1._tcp.local                            4500     2         c869.cda8.77d6
vk11._custom1._tcp.local
_ipp._tcp.local                                4500     2         c869.cda8.77d6
service-4._ipp._tcp.local
```

To verify the mdns-sd cache for a client MAC, use the following command:

```
Device# show mdns-sd cache {ap-mac <ap-mac> | client-mac <client-mac> | glan-id <glan-id>
| mdns-ap <mac-address> | rlan-id <rlan-id> | wlan-id <wlan-id> | wired}
RECORD-NAME                                    TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------
```

```
_custom1._tcp.local                              4500     2         c869.cda8.77d6
service_t1._custom1._tcp.local
_custom1._tcp.local                              4500     2         c869.cda8.77d6
vk11._custom1._tcp.local
_ipp._tcp.local                                  4500     2         c869.cda8.77d6
service-4._ipp._tcp.local

------------------------------------------------------------ SRV Records
------------------------------------------------------------
RECORD-NAME                                      TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------
service-4._ipp._tcp.local                       4500     2         c869.cda8.77d6   0 0 1212
 mDNS-Client1s-275.local
vk11._custom1._tcp.local                         4500     2         c869.cda8.77d6   0 0 987
 mDNS-Client1s-275.local
service_t1._custom1._tcp.local                   4500     2         c869.cda8.77d6   0 0 197
 mDNS-Client1s-275.local

------------------------------------------------------------ A/AAAA Records
------------------------------------------------------------
RECORD-NAME                                      TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------
mDNS-Client1s-275.local                         4500     2         c869.cda8.77d6   120.1.1.33


------------------------------------------------------------ TXT Records
------------------------------------------------------------
RECORD-NAME                                      TTL      WLAN      CLIENT-MAC
RR-Record-Data
-------------------------------------------------------------------------------
service-4._ipp._tcp.local                       4500     2         c869.cda8.77d6   'CLient1'

vk11._custom1._tcp.local                         4500     2         c869.cda8.77d6
'txtvers=11'
service_t1._custom1._tcp.local                   4500     2         c869.cda8.77d6
'txtvers=12'
```

To verify the mdns-sd cache with respect to the RLAN ID, use the following command:

```
Device# show mdns-sd cache rlan-id 1 detail

Name: _printer._tcp.local

  Type: PTR
  TTL: 4500
  RLAN: 1
  RLAN Name: rlan_test_1
  VLAN: 141
  Client MAC: 000e.c688.3942
  AP Ethernet MAC: 0042.5ab6.0ef0
  Remaining-Time: 4485
  Site-Tag: default-site-tag
  mDNS Service Policy: mdnsTV6
  Overriding mDNS Service Policy: NO
  UPN-Status: Disabled
  Rdata: printer._printer._tcp.local

Name: lab-47-187.local
  Type: A/AAAA
  TTL: 4500
  RLAN: 1
  RLAN Name: rlan_test_1
  VLAN: 141
```

```
  Client MAC: 000e.c688.3942
  AP Ethernet MAC: 0042.5ab6.0ef0
  Remaining-Time: 4485
  Site-Tag: default-site-tag
  mDNS Service Policy: mdnsTV6
  Overriding mDNS Service Policy: NO
  UPN-Status: Disabled
  Rdata: 10.15.141.124
```

To verify the mdns-sd cache with respect to mDNS-AP, use the following command:

```
Device# show mdns-sd cache mdns-ap 706b.b97d.b060 detail
Name: _printer._tcp.local

  Type: PTR
  TTL: 4500
  VLAN: 145
  Client MAC: 0050.b626.5bfa
  mDNS AP Radio MAC: 706b.b97d.b060
  mDNS AP Ethernet MAC: 706b.b97c.5208
  Remaining-Time: 4480
  mDNS Service Policy: mdnsTV
  Rdata: printer._printer._tcp.local

Name: Client-46-153.local
  Type: A/AAAA
  TTL: 4500
  VLAN: 145
  Client MAC: 0050.b626.5bfa
  mDNS AP Radio MAC: 706b.b97d.b060
  mDNS AP Ethernet MAC: 706b.b97c.5208
  Remaining-Time: 4480
  mDNS Service Policy: mdnsTV
  Rdata: 10.15.145.103
```

To verify the mdns-sd cache in detail, use the following command:

```
Device# show mdns-sd cache detail

Name: _custom1._tcp.local
  Type: PTR
  TTL: 4500
  WLAN: 2
  WLAN Name: mdns120
  VLAN: 120
  Client MAC: c869.cda8.77d6
  AP Ethernet MAC: 7069.5ab8.33d0
  Expiry-Time: 09/09/18 21:50:47
  Site-Tag: default-site-tag
  Rdata: service_t1._custom1._tcp.local
```

To verify the mdns-sd cache statistics, use the following command:

```
Device# show mdns-sd cache statistics

mDNS Cache Stats

Total number of Services: 4191
```

To verify the mdns-sd statistics, use the following command:

```
Device# show mdns-sd statistics

---------------------------------------------------------
```

```
Consolidated mDNS Packet Statistics
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 61045
  IPv4 sent: 30790
    IPv4 advertisements sent: 234
    IPv4 queries sent: 30556
  IPv6 sent: 30255
    IPv6 advertisements sent: 17
    IPv6 queries sent: 30238
  Multicast sent: 57558
    IPv4 sent: 28938
    IPv6 sent: 28620
mDNS packets received: 72796
  advertisements received: 13604
  queries received: 59192
  IPv4 received: 40600
    IPv4 advertisements received: 6542
    IPv4 queries received: 34058
  IPv6 received: 32196
    IPv6 advertisements received: 7062
    IPv6 queries received: 25134
mDNS packets dropped: 87

-----------------------------------------------------
Wired mDNS Packet Statistics
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 61033
  IPv4 sent: 30778
    IPv4 advertisements sent: 222
    IPv4 queries sent: 30556
  IPv6 sent: 30255
    IPv6 advertisements sent: 17
    IPv6 queries sent: 30238
  Multicast sent: 57558
    IPv4 sent: 28938
    IPv6 sent: 28620
mDNS packets received: 52623
  advertisements received: 1247
  queries received: 51376
  IPv4 received: 32276
    IPv4 advertisements received: 727
    IPv4 queries received: 31549
  IPv6 received: 20347
    IPv6 advertisements received: 520
    IPv6 queries received: 19827
mDNS packets dropped: 63

-----------------------------------------------------
mDNS Packet Statistics, for WLAN: 2
-----------------------------------------------------
mDNS stats last reset time: 03/11/19 04:17:35
mDNS packets sent: 12
  IPv4 sent: 12
    IPv4 advertisements sent: 12
    IPv4 queries sent: 0
  IPv6 sent: 0
    IPv6 advertisements sent: 0
    IPv6 queries sent: 0
  Multicast sent: 0
    IPv4 sent: 0
    IPv6 sent: 0
mDNS packets received: 20173
```

```
  advertisements received: 12357
  queries received: 7816
  IPv4 received: 8324
    IPv4 advertisements received: 5815
    IPv4 queries received: 2509
  IPv6 received: 11849
    IPv6 advertisements received: 6542
    IPv6 queries received: 5307
mDNS packets dropped: 24
```

To verify the default service list details, use the following command:

```
Device# show mdns-sd default-service-list
-----------------------------------------
mDNS Default Service List
-----------------------------------------

Service Definition: apple-tv
Service Names: _airplay._tcp.local
_raop._tcp.local

Service Definition: homesharing
Service Names: _home-sharing._tcp.local

Service Definition: printer-ipps
Service Names: _ipps._tcp.local

Service Definition: apple-airprint
Service Names: _ipp._tcp.local
_universal._sub._ipp._tcp.local

Service Definition: google-chromecast
Service Names: _googlecast._tcp.local
_googlerpc._tcp.local
_googlezone._tcp.local

Service Definition: apple-remote-login
Service Names: _sftp-ssh._tcp.local
_ssh._tcp.local

Service Definition: apple-screen-share
Service Names: _rfb._tcp.local

Service Definition: google-expeditions
Service Names: _googexpeditions._tcp.local

Service Definition: multifunction-printer
Service Names: _fax-ipp._tcp.local
_ipp._tcp.local
_scanner._tcp.local

Service Definition: apple-windows-fileshare
Service Names: _smb._tcp.local
```

To verify the primary service list details, use the following command:

```
Device# show mdns-sd master-service-list

-----------------------------------------
        mDNS Master Service List
-----------------------------------------

Service Definition: fax
Service Names: _fax-ipp._tcp.local
```

```
Service Definition: roku
Service Names: _rsp._tcp.local

Service Definition: airplay
Service Names: _airplay._tcp.local

Service Definition: scanner
Service Names: _scanner._tcp.local

Service Definition: spotify
Service Names: _spotify-connect._tcp.local

Service Definition: airtunes
Service Names: _raop._tcp.local

Service Definition: airserver
Service Names: _airplay._tcp.local
               _airserver._tcp.local

.
.
.

Service Definition: itune-wireless-devicesharing2
Service Names: _apple-mobdev2._tcp.local
```

To verify the mdns-sd service statistics on the controller, use the following command:

```
Device# show mdns-sd service statistics

Service Name                                                              Service Count
------------------------------------------------------------------------------------
_atc._tcp.local                                                            137
_hap._tcp.local                                                            149
_ipp._tcp.local                                                            149
_rfb._tcp.local                                                            141
_smb._tcp.local                                                            133
_ssh._tcp.local                                                            142
_daap._tcp.local                                                           149
_dpap._tcp.local                                                           149
_eppc._tcp.local                                                           138
_adisk._tcp.local                                                          149
```

To verify the mDNS-AP configured on the controller and VLAN(s) associated with it, use the following command:

```
Device# show mdns-sd ap

Number of mDNS APs.............................. 1

AP Name   Ethernet MAC   Number of Vlans   Vlanidentifiers
-------------------------------------------------------------------------------------------------------
AP3600-1   7069.5ab8.33d0          1      300
```

Further Debug

To debug mDNS further, use the following procedure:

1. Run this command at the controller:

   ```
   set platform software trace wncd <0-7> chassis active R0 mdns debug
   ```

2. Reproduce the issue.

3. Run this command to gather the traces enabled:

```
show wireless loadbalance ap affinity wncd 0

AP MAC   Discovery Timestamp  Join Timestamp               Tag    Vlanidentifiers
-------------------------------------------------------------------------------------
0cd0.f894.0600      06/30/21 12:39:48    06/30/21 12:40:021 default-site-tag     300
```