Software-Defined Access Wireless for Catalyst 4500E Series Switches, Cisco IOS XE 3.10.0E

First Published: 2017-08-08

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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation. This chapter includes the following sections:

Audience

This publication is for experienced network administrators who configure and maintain the Cisco Catalyst 4500E Switches.

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
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.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Indication
string	A nonquoted set of characters. Do not use quotation marks around the string. Otherwise, the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	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.

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 perform an action that could result in equipment damage or loss of data.

Related Documentation

Note Before installing or upgrading the device, refer to the device release notes.

- Cisco Catalyst 4500 Series Switch documentation:

  https://www.cisco.com/c/en/us/support/switches/catalyst-4500-series-switches/tsd-products-support-series-home.html

- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:

  https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/tsd-products-support-series-home.html

- Cisco SFP, SFP+, and QSFP+ modules documentation, including compatibility matrixes, located at:

  https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/tsd-products-support-series-home.html

- Cisco Validated Designs documents, located at:

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

- Error Message Decoder, located at::

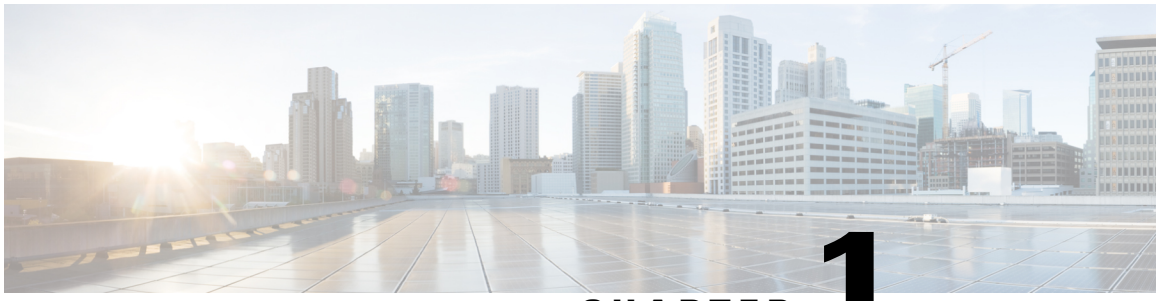
https://www.cisco.com/c/en/us/support/web/tools/help/error_message_search_best_practices.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Software-Defined Access Wireless

Introduction 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.

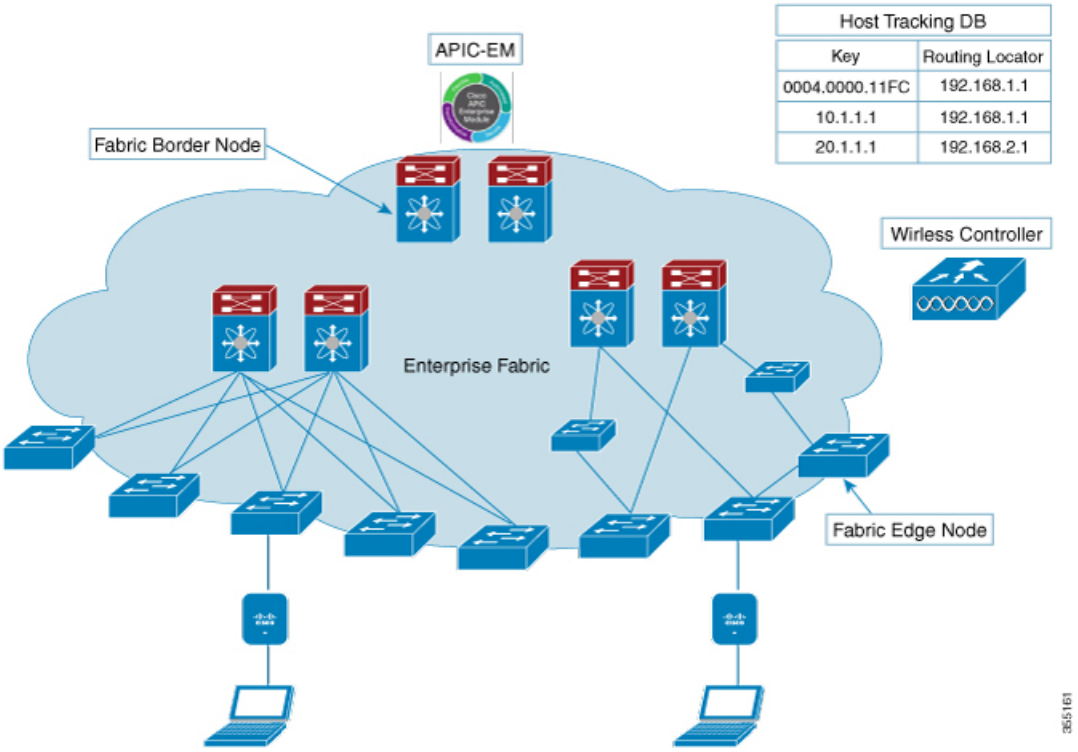
Enterprise fabric is a network topology where traffic is passed through inter-connected switches, while providing the abstraction of a single Layer 2 or Layer 3 device. This provides seamless connectivity, with policy application and enforcement at the edge of the fabric. Fabric uses IP overlay, which 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 (WLC), Application Policy Infrastructure Controller - Enterprise Module (APIC-EM), and Host Tracking Database (HDB).

Figure 1: Software-Defined Access Wireless



APIC-EM Controller: Fabric service, developed on the APIC-EM controller, drives the management and orchestration of enterprise fabric. It also provisions policies for attached users and devices.

Host ID Tracking Database(map-server and map-resolver in LISP): 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 WLC 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, etc. It establishes CAPWAP control and data tunnel to WLC. 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

AP Bring-up Process

The sequence of bringing up an AP is given below:

- Switch powers up the AP (POE or UPOE)
- AP gets an IP address from the DHCP server.
- Switch registers the IP address of the AP with the map server.
- AP discovers Cisco WLC through CAPWAP discovery.
- After Datagram Transport Layer Security (DTLS) handshake, CAPWAP control tunnel is created between AP and Cisco WLC for control packets. CAPWAP data tunnel is created for IEEE 802.11 management frames. The AP image is downloaded and the configuration is pushed on AP from controller.
- Cisco WLC queries the map server for the switch (RLOC IP) behind which the AP has been registered.
- Cisco WLC registers a dummy MAC address with the map server.
- Map server sends a dummy MAC address notification to the switch to create a VXLAN tunnel to AP.
- AP is ready to accept clients.

Onboarding the Wireless Clients

The sequence of on boarding the clients are given below:

- The wireless client associates itself to the AP.
- Client starts IEEE 802.1x authentication on Cisco WLC (if configured) using CAPWAP data tunnel.
- After Layer 2 authentication is complete, Cisco WLC registers MAC address of the client with map server.
- Map server sends a notify message to switch with the client details.
- Switch adds the client mac to the Layer 2 forwarding table.

- Client gets an IP address from DHCP server.
- AP sends IP address of the client to Cisco WLC.
- Cisco WLC moves the client to RUN state and the client can start sending traffic.
- Switch registesr the IP address of the client to the MAP server.
- The switch decapsulates the VXLAN packet.
- The switch forwards the DHCP packet to the DHCP server or relay.
- The switch receives the DHCP ack for the wireless client. Switch learns the IP address of the client and sends an update to the map server.
- Switch broadcasts the DHCP ack to all ports in the VLAN, including the AP facing VXLAN tunnels.
- DHCP ack reaches AP, which forwards it to client.
- AP sends IP address of the client to WLC.
- Cisco WLC puts the client in RUN state.

Platform Support

Table 2: Supported AireOS Controllers

Controller	Support
2504	No
3504	Yes
5508	No
WiSM2	No
8510	Supported only on the local mode AP
5520	Supported only on the local mode AP
8540	Supported only on the local mode AP
7510	No
vWLC	No

Table 3: AP Support

AP	Support
11N	No

AP	Support
11AC Wave 1	Yes
11AC Wave 2	Yes
Mesh	No

Table 4: Client Security

Security	Support
Open and Static WEP	No
WPA-PSK	Yes
802.1x (WPA/WPA2)	Yes
MAC Filtering	Yes
CCKM Fast Roaming	Yes
Local EAP	Yes. However, it is not recommended.
AAA Override	Supported for SGT, L2 VNID, ACL policy, and QoS policy.
Internal WebAuth	IPv4 clients
External Webauth	IPv4 clients
Pre Auth ACL	IPv4 clients
FQDN ACL	No

Table 5: IPv6 Support

IPv6	Support
IPv6 Infra Support	No
IPv6 Client Support	No

Table 6: Polciy, QoS, and Feature Support

Features	Support
IPv4 ACL for Clients	Yes. Flex ACL for ACL at AP.
IPv6 ACL for Clients	No
P2P Blocking	Supported through security group tag (SGT) and security group ACL (SGACL) on the switch for clients on the same AP.
IP Source Guard	Switches
AVC Visibility	AP
AVC QOS	AP
Downloadable Protocol Pack updates	No
Device profiling	No
mDNS Proxy	No
MS Lync Server QOS Integration	No
Netflow Exporter	No
QOS	Yes (Metal profiles and rate limiting)
Passive Client/Silent Host	No
Location tracking / Halo	Yes
Wireless Multicast	Yes. Video streaming is not supported.
URL Filtering	No
HA	WLC to WLC

Migration From Converged Access

The following list shows the migration process from converged access to fabric wireless:

1. Bring up the WLC with image supporting fabric mode.
2. Configure the network with the fabric mode for the appropriate subnets, using an APIC-EM or CLIs. We recommed that you use APIC-EM for this purpose.

3 Configure the discovery mechanism such that the DHCP discovery on the new AP subnet should lead to the controller supporting fabric mode.

4 When the AP comes up, do a DHCP request and get the IP address in the AP VLAN.

5 The AP creates a control plane CAPWAP tunnel with the WLC.

6 Based on the configuration, the WLC programs the AP for the fabric mode.

7 After this, AP follows the SDA for wireless flow.

Note Mobility between fabric and non-fabric SSIDs are not supported

Note AP images and licenses are hosted on the Cisco WLC and the AP fetches the images and licenses directly from it. APIC-EM is responsible for managing the AP licenses on the Cisco WLC.

Note After a TCP connection flap in the WLC, it takes about five to six minutes to reestablish the connection. During this time, the access tunnels gets reset during client join.

Configuring SD-Access Wireless (CLI)

Perform the following steps to configure fabric on a WLAN.

Before You Begin

- Configure the AP in local mode to enable fabric on it.

Step 1 **config wlan fabric enable** *wlanid*

Example:
```
config wlan fabric enable wlan1
```
Enables Fabric on the WLAN.

Step 2 **config wlan fabric vnid** *vnid wlanid*

Example:
```
config wlan fabric vnid 10 wlan1
```
Configures a Virtual Extensible LAN (VXLAN) network identifier (VNID) on fabric WLAN.

Step 3 **config wlan fabric encap vxlan** *wlanid*

Example:
```
config wlan fabric encap vxlan wlan1
```
Maps a VNID to the fabric WLAN.

Step 4 **config wlan fabric switch-ip** *ip-address wlanid*

Example:
```
config wlan fabric switch-ip 1.1.1.1 wlan1
```
Sets a VLAN peer ip to WLAN.

Step 5 **config wlan fabric acl** *fabric-acl-name wlanid*

Example:
```
config wlan fabric acl fabric-acl wlan1
```
Configures a flex ACL on the WLC and associates it with the fabric WLAN.

Step 6 **config wlan fabric avc-policy** *fabric-avc-policy wlanid*

Example:
```
config wlan fabric fabric-avc-policy wlan1
```
Configures an AVC profile name associates it with the fabric WLAN.

Step 7 **config wlan fabric controlplane guest-fabric enable** *wlanid*

Example:
```
config wlan fabric controlplane guest-fabric enable wlan1
```
(Optional) Enables guest fabric for this WLAN .

Step 8 **show fabric summary**

Example:
```
show fabric summary
```
(Optional) Displays the fabric configuration summary.

Enabling SD-Access Wireless (GUI)

Use the following procedure to enable fabric and configure parameters on the enterprise and guest controllers.

Step 1 Choose **Controller > Fabric Configuration > Control Plane**.
The Fabric Control Configuration page is displayed.

Step 2 Move the Fabric slider to enable or disable Fabric.
You can enable fabric and configure parameters on the enterprise and guest controllers, using the Fabric Enable/Disable option at the top of the screen.

Step 3 Select the check box in the Primary IP Address field to enable the fields.
Step 4 Enter an IP address in the **Primary IP Address** field.
Step 5 Enter a shared key in the **Pre Shared Key** field.
Step 6 The **Connection Status** field shows the connection status of the Fabric.
Step 7 Repeat the procedure described in steps 3 to 6 for **Secondary IP Address** and in the **Guest Controllers** section.
Step 8 Click **Apply**.

Configuring SD-Access Wireless VNID (GUI)

Use the following procedure to enable fabric and configure parameters on the enterprise and guest controllers.

Step 1 Choose **Controller > Fabric Configuration > Interface**.
The **Fabric Interface > Edit** page is displayed.
Step 2 Enter an interface name in the **Fabric Interface Name** field.
Step 3 Enter an instance ID in the **L2 Instance ID** field.
Step 4 Enter the network IP adddress in the **Network IP** field.
Step 5 Enter the subnet mask at the **Subnet Massk** field.
Step 6 Enter an instance ID in the **L3 Instance ID** field.
Step 7 Click **Apply**.

Configuring SD-Access Wireless WLAN (GUI)

Use the following procedure to configure Fabric WLAN parameters.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** page.

Step 3 Choose the **Advanced** tab to open the **WLANs > Edit (Advanced)** page.

Step 4 Select the Enabled check box under the Fabric Configuration section.

Step 5 Use the drop down to select the **Fabric Interface Name**.

Step 6 Enter an instance ID in the **L2 Instance ID** field.

Step 7 Enter the IP adddress in the **Peer IP** field.

Step 8 Use the drop down to select the **Fabric ACL** name.

Step 9 Use the drop down to select the **Fabric AVC** name.

Step 10 Click **Apply**.