Cisco Wireless Controller リリース 8.2 コマンド リファレンス

初版：2015 年 11 月 30 日

最終更新：2018 年 12 月 7 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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: 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. (1721R)

© 2015 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに li

対象読者 li

表記法 li

関連資料 liv

マニュアルの入手方法およびテクニカル サポート liv

第 I 部：

コマンドライン インターフェイスの使用 55

第 1 章

コマンドライン インターフェイスの使用 1

CLI コマンドのキーボード ショートカット 2

対話型ヘルプ機能の使用 4

help コマンドの使用方法 4

? コマンドの使用方法 5

コマンドの一部と ? の使用法 5

コマンド名の一部と <tab> の使用法 6

コマンドと ? の使用法 6

コマンド キーワード? 7

第 II 部：

clear コマンド 9

第 2 章

clear コマンド：a ～ l 11

clear advanced 12

clear acl counters 13

clear ap config 14

clear ap eventlog 15

clear ap join stats 16
clear arp 17
clear ap tsm 18
clear atf 19
clear avc statistics 20
clear client tsm 22
clear config 23
clear ext-webauth-url 24
clear location rfid 25
clear location statistics rfid 26
clear locp statistics 27
clear login-banner 28
clear lwapp private-config 29

第 3 章 clear コマンド：m ～ z 31
clear mdns service-database 32
clear nmsp statistics 33
clear radius acct statistics 34
clear session 35
clear tacacs auth statistics 36
clear redirect-url 37
clear stats ap wlan 38
clear stats local-auth 39
clear stats mobility 40
clear stats port 41
clear stats radius 42
clear stats smart-lic 44
clear stats switch 45
clear stats tacacs 46
clear transfer 47
clear traplog 48
clear webimage 49
clear webmessage 50
clear webtitle 51

第 III 部 : コンフィギュレーション コマンド 53

第 4 章 **config コマンド : 802.11** 55

config 802.11-abgn 58
config 802.11a 11acsupport 59
config 802.11-a antenna extAntGain 60
config 802.11-a channel ap 61
config 802.11-a txpower ap 62
config 802.11 antenna diversity 63
config 802.11 antenna extAntGain 64
config 802.11 antenna mode 65
config 802.11 antenna selection 66
config 802.11b 11gSupport 67
config 802.11b preamble 68
config 802.11h channelswitch 69
config 802.11h powerconstraint 70
config 802.11h setchannel 71
config 802.11 11nsupport 72
config 802.11 11nsupport a-mpdu tx priority 73
config 802.11 11nsupport a-mpdu tx scheduler 75
config 802.11 11nsupport antenna 76
config 802.11 11nsupport guard-interval 77
config 802.11 11nsupport mcs tx 78
config 802.11 11nsupport rifs 80
config 802.11 antenna diversity 81
config 802.11 antenna extAntGain 82
config 802.11 antenna mode 83
config 802.11 antenna selection 84
config 802.11 channel 85
config 802.11 channel ap 87
config 802.11 chan_width 88
config 802.11 rx-sop threshold 90
config 802.11 txPower 92

config 802.11 beamforming 94
config 802.11h channelswitch 96
config 802.11h powerconstraint 97
config 802.11h setchannel 98
config 802.11h smart dfs 99
config 802.11 11nsupport 100
config 802.11 11nsupport a-mpdu tx priority 101
config 802.11 11nsupport a-mpdu tx scheduler 103
config 802.11 11nsupport antenna 104
config 802.11 11nsupport guard-interval 105
config 802.11 11nsupport mcs tx 106
config 802.11 11nsupport rifs 108
config 802.11 beacon period 109
config 802.11 cac defaults 110
config 802.11 cac video acm 112
config 802.11 cac video cac-method 114
config 802.11 cac video load-based 116
config 802.11 cac video max-bandwidth 118
config 802.11 cac media-stream 120
config 802.11 cac multimedia 122
config 802.11 cac video roam-bandwidth 124
config 802.11 cac video sip 126
config 802.11 cac video tspec-inactivity-timeout 128
config 802.11 cac voice acm 130
config 802.11 cac voice max-bandwidth 132
config 802.11 cac voice roam-bandwidth 134
config 802.11 cac voice tspec-inactivity-timeout 136
config 802.11 cac voice load-based 138
config 802.11 cac voice max-calls 140
config 802.11 cac voice sip bandwidth 142
config 802.11 cac voice sip codec 144
config 802.11 cac voice stream-size 146
config 802.11 cleanair 148
config 802.11 cleanair device 151

config 802.11 cleanair alarm 153
config 802.11 disable 155
config 802.11 dtpc 156
config 802.11 enable 157
config 802.11 exp-bwreq 159
config 802.11 fragmentation 160
config 802.11 l2roam rf-params 161
config 802.11 max-clients 164
config 802.11 media-stream multicast-direct 165
config 802.11 media-stream video-redirect 167
config 802.11 multicast data-rate 168
config 802.11 rate 169
config 802.11 rssi-check 171
config 802.11 rssi-threshold 172
config 802.11 tsm 173
config 802.11b preamble 174

第 5 章 **config コマンド：a ～ i** 175
config aaa auth 183
config aaa auth mgmt 184
config acl apply 185
config acl counter 186
config acl create 187
config acl cpu 188
config acl delete 189
config acl layer2 190
config acl rule 192
config acl url-domain 194
config advanced 802.11 7920VSIEConfig 195
config advanced 802.11 channel add 196
config advanced 802.11 channel cleanair-event 197
config advanced 802.11 channel dca anchor-time 198
config advanced 802.11 channel dca chan-width-11n 199
config advanced 802.11 channel dca interval 200

config advanced 802.11 channel dca min-metric 201
config advanced 802.11 channel dca sensitivity 202
config advanced 802.11 channel foreign 204
config advanced 802.11 channel load 205
config advanced 802.11 channel noise 206
config advanced 802.11 channel outdoor-ap-dca 207
config advanced 802.11 channel pda-prop 208
config advanced 802.11 channel update 209
config advanced 802.11 coverage 210
config advanced 802.11 coverage exception global 212
config advanced 802.11 coverage fail-rate 213
config advanced 802.11 coverage level global 215
config advanced 802.11 coverage packet-count 216
config advanced 802.11 coverage rssi-threshold 218
config advanced 802.11 edca-parameters 220
config advanced 802.11 factory 223
config advanced 802.11 group-member 224
config advanced 802.11 group-mode 225
config advanced 802.11 logging channel 226
config advanced 802.11 logging coverage 227
config advanced 802.11 logging foreign 228
config advanced 802.11 logging load 229
config advanced 802.11 logging noise 230
config advanced 802.11 logging performance 231
config advanced 802.11 logging txpower 232
config advanced 802.11 monitor channel-list 233
config advanced 802.11 monitor load 234
config advanced 802.11 monitor measurement 235
config advanced 802.11 monitor mode 236
config advanced 802.11 monitor ndp-type 237
config advanced 802.11 monitor timeout-factor 238
config advanced 802.11 optimized roaming 239
config advanced 802.11 packet 241
config advanced 802.11 profile clients 243

config advanced 802.11 profile customize 244
config advanced 802.11 profile foreign 245
config advanced 802.11 profile noise 246
config advanced 802.11 profile throughput 247
config advanced 802.11 profile utilization 248
config advanced 802.11 receiver 249
config advanced 802.11 reporting measurement 250
config advanced 802.11 tpc-version 251
config advanced 802.11 tpcv1-thresh 252
config advanced 802.11 tpcv2-intense 253
config advanced 802.11 tpcv2-per-chan 254
config advanced 802.11 tpcv2-thresh 255
config advanced 802.11 txpower-update 256
config advanced eap 257
config advanced hotspot 260
config advanced timers auth-timeout 262
config advanced timers eap-timeout 263
config advanced timers eap-identity-request-delay 264
config advanced timers 265
config advanced fastpath fastcache 268
config advanced fastpath pkt-capture 269
config advanced sip-preferred-call-no 270
config advanced sip-snooping-ports 271
config advanced backup-controller primary 272
config advanced backup-controller secondary 273
config advanced client-handoff 274
config advanced dot11-padding 275
config advanced assoc-limit 276
config advanced max-1x-sessions 277
config advanced rate 278
config advanced probe backoff 279
config advanced probe filter 280
config advanced probe limit 281
config advanced timers 282

config ap 802.1Xuser 285
config ap 802.1Xuser delete 286
config ap 802.1Xuser disable 287
config advanced dot11-padding 288
config ap 289
config ap aid-audit 290
config ap antenna band-mode 291
config ap atf 802.11 292
config ap atf 802.11 policy 293
config ap autoconvert 294
config ap bhrate 295
config ap bridgegroupname 296
config ap bridging 297
config ap cdp 298
config ap core-dump 300
config ap crash-file clear-all 301
config ap crash-file delete 302
config ap crash-file get-crash-file 303
config ap crash-file get-radio-core-dump 304
config ap dtls-cipher-suite 305
config ap ethernet duplex 306
config ap ethernet tag 307
config ap autoconvert 308
config ap flexconnect bridge 309
config ap flexconnect central-dhcp 310
config ap flexconnect local-split 312
config ap flexconnect module-vlan 313
config ap flexconnect policy 314
config ap flexconnect radius auth set 315
config ap flexconnect vlan 316
config ap flexconnect vlan add 317
config ap flexconnect vlan native 318
config ap flexconnect vlan wlan 319
config ap flexconnect web-auth 320

config ap flexconnect web-policy acl 321
config ap flexconnect wlan 322
config ap group-name 323
config ap hotspot 324
config ap image predownload 331
config ap image swap 332
config ap lag-mode support 333
config ap led-state 334
config ap link-encryption 335
config ap link-latency 336
config ap location 337
config ap logging syslog level 338
config ap logging syslog facility 339
config ap max-count 342
config ap mgmtuser add 343
config ap mgmtuser delete 345
config ap mode 346
config ap module3g 348
config ap monitor-mode 349
config ap name 350
config ap packet-dump 351
config ap port 355
config ap power injector 356
config ap power pre-standard 357
config ap preferred-mode 358
config ap primary-base 359
config ap priority 361
config ap reporting-period 362
config ap reset 363
config ap retransmit interval 364
config ap retransmit count 365
config ap role 366
config ap rst-button 367
config ap secondary-base 368

config ap slub-debug 370
config ap sniff 372
config ap ssh 374
config ap static-ip 375
config ap stats-timer 377
config ap syslog host global 378
config ap syslog host specific 379
config ap tcp-mss-adjust 380
config ap telnet 381
config ap tertiary-base 382
config ap tftp-downgrade 384
config ap username 385
config ap venue 386
config ap wlan 390
config atf 802.11 391
config atf policy 392
config auth-list add 393
config auth-list ap-policy 394
config auth-list delete 395
config avc profile create 396
config avc profile delete 397
config avc profile rule 398
config band-select cycle-count 400
config band-select cycle-threshold 401
config band-select expire 402
config band-select client-rssi 403
config boot 404
config call-home contact email address 405
config call-home events 406
config call-home http-proxy ipaddr 407
config call-home http-proxy ipaddr 0.0.0.0 408
config call-home profile 409
config call-home profile delete 410
config call-home profile status 411

config call-home reporting 412
config call-home tac-profile 413
config cdp 414
config certificate lsc 415
config certificate ssc 418
config certificate use-device-certificate webadmin 420
config client ccx clear-reports 421
config client ccx clear-results 422
config client ccx default-gw-ping 423
config client ccx dhcp-test 424
config client ccx dns-ping 425
config client ccx dns-resolve 426
config client ccx get-client-capability 427
config client ccx get-manufacturer-info 428
config client ccx get-operating-parameters 429
config client ccx get-profiles 430
config client ccx log-request 431
config client ccx send-message 433
config client ccx stats-request 437
config client ccx test-abort 438
config client ccx test-association 439
config client ccx test-dot1x 440
config client ccx test-profile 441
config client deauthenticate 442
config client location-calibration 443
config client profiling delete 444
config coredump 445
config coredump ftp 446
config coredump username 447
config country 448
config cts sxp 449
config custom-web ext-webauth-mode 451
config custom-web ext-webauth-url 452
config custom-web ext-webserver 453

config custom-web logout-popup 454
config custom-web radiusauth 455
config custom-web redirectUrl 456
config custom-web sleep-client 457
config custom-web webauth-type 458
config custom-web weblogo 459
config custom-web webmessage 460
config custom-web webtitle 461
config database size 462
config dhcp 463
config dhcp opt-82 format 466
config dhcp opt-82 remote-id 467
config dhcp proxy 469
config dhcp timeout 470
config exclusionlist 471
config flexconnect [ipv6] acl 472
config flexconnect [ipv6] acl rule 473
config flexconnect [ipv6] acl url-domain 475
config flexconnect arp-caching 476
config flexconnect avc profile 477
config flexconnect fallback-radio-shut 478
config flexconnect group 479
config flexconnect group vlan 485
config flexconnect group group-name dhcp overridden-interface 486
config flexconnect group web-auth 487
config flexconnect group web-policy 488
config flexconnect join min-latency 489
config flexconnect office-extend 490
config flow 492
config guest-lan 493
config guest-lan custom-web ext-webauth-url 494
config guest-lan custom-web global disable 495
config guest-lan custom-web login_page 496
config guest-lan custom-web webauth-type 497

config guest-lan ingress-interface 498
config guest-lan interface 499
config guest-lan mobility anchor 500
config guest-lan nac 501
config guest-lan security 502
config interface 3g-vlan 503
config interface acl 504
config interface address 505
config interface address redundancy-management 507
config interface ap-manager 508
config interface create 509
config interface delete 510
config interface dhcp management 511
config interface dhcp 513
config interface address 514
config interface guest-lan 516
config interface hostname 517
config interface nasid 518
config interface nat-address 519
config interface port 520
config interface quarantine vlan 521
config interface vlan 522
config interface group mdns-profile 523
config interface mdns-profile 525
config icons delete 527
config icons file-info 528
config ipv6 disable 529
config ipv6 enable 530
config ipv6 acl 531
config ipv6 capwap 533
config ipv6 interface 534
config ipv6 interface multicast 536
config ipv6 neighbor-binding 537
config ipv6 na-mcast-fwd 539

config ipv6 ns-mcast-fwd 540
config ipv6 ra-guard 541
config ipv6 route 542

第 6 章

config コマンド：j ～ q 543
config known ap 549
config lag 550
config ldap 551
config local-auth active-timeout 553
config local-auth cipher-option 554
config local-auth eap-profile 555
config local-auth method fast 558
config local-auth user-credentials 560
config lync-sdn 561
config licensing 562
config license boot 563
config load-balancing 565
config location 567
config location info rogue 570
config logging buffered 571
config logging console 572
config logging debug 573
config logging fileinfo 574
config logging procinfo 575
config logging traceinfo 576
config logging syslog host 577
config logging syslog facility 580
config logging syslog facility client 584
config logging syslog facility ap 585
config logging syslog level 586
config loginsession close 587
config macfilter 588
config macfilter description 590
config macfilter interface 591

config macfilter ip-address 592
config macfilter mac-delimiter 593
config macfilter radius-compat 594
config macfilter wlan-id 595
config mdns ap 596
config mdns profile 598
config mdns query interval 600
config mdns service 601
config mdns snooping 604
config mdns policy enable 605
config mdns policy service-group 606
config mdns policy service-group parameters 607
config mdns policy service-group user-name 608
config mdns policy service-group user-role 609
config media-stream multicast-direct 610
config media-stream message 611
config media-stream add 613
config media-stream admit 615
config media-stream deny 616
config media-stream delete 617
config memory monitor errors 618
config memory monitor leaks 619
config mesh alarm 621
config mesh astools 623
config mesh backhaul rate-adapt 624
config mesh backhaul slot 626
config mesh battery-state 627
config mesh client-access 628
config mesh convergence 630
config mesh ethernet-bridging allow-bpdu 631
config mesh ethernet-bridging vlan-transparent 632
config mesh full-sector-dfs 633
config mesh linkdata 634
config mesh linktest 637

config mesh lsc 640
config mesh lsc advanced 641
config mesh lsc advanced ap-provision 642
config mesh multicast 643
config mesh parent preferred 645
config mesh public-safety 646
config mesh radius-server 647
config mesh range 648
config mesh secondary-backhaul 649
config mesh security 650
config mesh slot-bias 652
config mgmtuser add 653
config mgmtuser delete 654
config mgmtuser description 655
config mgmtuser password 656
config mgmtuser telnet 657
config mgmtuser termination-interval 658
config mobility dscp 659
config mobility group anchor 660
config mobility group domain 661
config mobility group keepalive count 662
config mobility group keepalive interval 663
config mobility group member 664
config mobility group multicast-address 666
config mobility multicast-mode 667
config mobility new-architecture 668
config mobility oracle 669
config mobility secure-mode 670
config mobility statistics reset 671
config netuser add 672
config netuser delete 674
config netuser description 675
config netuser guest-lan-id 676
config netuser guest-role apply 677

config netuser guest-role create 678
config netuser guest-role delete 679
config netuser guest-role qos data-rate average-data-rate 680
config netuser guest-role qos data-rate average-realtime-rate 681
config netuser guest-role qos data-rate burst-data-rate 682
config netuser guest-role qos data-rate burst-realtime-rate 683
config netuser lifetime 684
config netuser maxUserLogin 685
config netuser password 686
config netuser wlan-id 687
config network client-ip-conflict-detection 688
config network bridging-shared-secret 689
config network web-auth captive-bypass 690
config network web-auth port 691
config network web-auth proxy-redirect 692
config network web-auth secureweb 693
config network webmode 694
config network web-auth 695
config network 802.3-bridging 696
config network allow-old-bridge-aps 697
config network ap-discovery 698
config network ap-fallback 699
config network ap-priority 700
config network apple-talk 701
config network arptimeout 702
config assisted-roaming 703
config network bridging-shared-secret 704
config network broadcast 705
config network fast-ssid-change 706
config network ip-mac-binding 707
config network link local bridging 708
config network master-base 709
config network mgmt-via-wireless 710
config network multicast global 711

config network multicast igmp query interval 712
config network multicast igmp snooping 713
config network multicast igmp timeout 714
config network multicast l2mcast 715
config network multicast mld 716
config network multicast mode multicast 717
config network multicast mode unicast 718
config network oeap-600 dual-rlan-ports 719
config network oeap-600 local-network 720
config network otap-mode 721
config network profiling 722
config pmipv6 domain 723
config pmipv6 add profile 724
config pmipv6 delete 725
config pmipv6 mag apn 726
config pmipv6 mag binding init-retx-time 727
config pmipv6 mag binding lifetime 728
config pmipv6 mag binding max-retx-time 729
config pmipv6 mag binding maximum 730
config pmipv6 mag binding refresh-time 731
config pmipv6 mag bri delay 732
config pmipv6 mag bri retries 733
config pmipv6 mag lma 734
config pmipv6 mag replay-protection 735
config port power 736
config network rf-network-name 737
config network secureweb 738
config network secureweb cipher-option 739
config network ssh 741
config network telnet 742
config network usertimeout 743
config network web-auth captive-bypass 744
config network web-auth cmcc-support 745
config network web-auth port 746

config network web-auth proxy-redirect 747
config network web-auth secureweb 748
config network web-auth https-redirect 749
config network webcolor 750
config network webmode 751
config network web-auth 752
config network zero-config 753
config network allow-old-bridge-aps 754
config network ap-discovery 755
config network ap-fallback 756
config network ap-priority 757
config network apple-talk 758
config network bridging-shared-secret 759
config network master-base 760
config network oeap-600 dual-rlan-ports 761
config network oeap-600 local-network 762
config network otap-mode 763
config network zero-config 764
config nmsp notify-interval measurement 765
config paging 766
config passwd-cleartext 767
config policy 768
config port adminmode 771
config port autoneg 772
config port linktrap 773
config port multicast appliance 774
config prompt 775
config qos average-data-rate 776
config qos average-realtime-rate 778
config qos burst-data-rate 780
config qos burst-realtime-rate 782
config qos description 784
config qos max-rf-usage 785
config qos dot1p-tag 786

config qos priority 787
config qos protocol-type 789
config qos queue_length 790
config qos qosmap 791
config qos qosmap up-to-dscp-map 792
config qos qosmap dscp-to-up-exception 793
config qos qosmap delete-dscp-exception 794
config qos qosmap clear-all 795
config qos qosmap trust dscp upstream 796

第 7 章 **config コマンド：r ～ z** 797
config radius acct 806
config radius acct ipsec authentication 810
config radius acct ipsec disable 811
config radius acct ipsec enable 812
config radius acct ipsec encryption 813
config radius acct ipsec ike 814
config radius acct mac-delimiter 815
config radius acct network 816
config radius acct realm 817
config radius acct retransmit-timeout 818
config radius auth 819
config radius auth callStationIdType 822
config radius auth framed-mtu 825
config radius auth IPsec authentication 826
config radius auth ipsec disable 827
config radius auth ipsec encryption 828
config radius auth ipsec ike 829
config radius auth keywrap 831
config radius auth mac-delimiter 832
config radius auth management 833
config radius auth mgmt-retransmit-timeout 834
config radius auth network 835
config radius auth realm 836

config radius auth retransmit-timeout 837
config radius auth rfc3576 838
config radius auth retransmit-timeout 839
config radius aggressive-failover disabled 840
config radius backward compatibility 841
config radius callStationIdCase 842
config radius callStationIdType 843
config radius dns 846
config radius fallback-test 848
config radius ext-source-ports 850
config radius acct retransmit-timeout 851
config radius auth mgmt-retransmit-timeout 852
config radius auth retransmit-timeout 853
config radius auth retransmit-timeout 854
config redundancy interface address peer-service-port 855
config redundancy mobilitymac 856
config redundancy mode 857
config redundancy peer-route 858
config redundancy timer keep-alive-timer 859
config redundancy timer peer-search-timer 860
config redundancy unit 861
config remote-lan 862
config remote-lan aaa-override 863
config remote-lan acl 864
config remote-lan create 865
config remote-lan custom-web 866
config remote-lan delete 869
config remote-lan dhcp_server 870
config remote-lan exclusionlist 871
config remote-lan interface 872
config remote-lan ldap 873
config remote-lan mac-filtering 874
config remote-lan mab 875
config remote-lan max-associated-clients 876

config remote-lan radius_server 877
config remote-lan security 879
config remote-lan session-timeout 880
config remote-lan webauth-exclude 881
config rf-profile band-select 882
config rf-profile channel 884
config rf-profile client-trap-threshold 885
config rf-profile create 886
config rf-profile fra client-aware 887
config rf-profile data-rates 888
config rf-profile delete 890
config rf-profile description 891
config rf-profile load-balancing 892
config rf-profile max-clients 894
config rf-profile multicast data-rate 895
config rf-profile out-of-box 896
config rf-profile rx-sop threshold 897
config rf-profile trap-threshold 898
config rf-profile tx-power-control-thresh-v1 899
config rf-profile tx-power-control-thresh-v2 900
config rf-profile tx-power-max 901
config rf-profile tx-power-min 902
config rogue ap timeout 903
config rogue adhoc 904
config rogue ap classify 908
config rogue ap friendly 910
config rogue ap rldp 912
config rogue ap ssid 914
config rogue ap timeout 916
config rogue auto-contain level 917
config rogue ap valid-client 919
config rogue client 921
config rogue containment 923
config rogue detection 924

config rogue detection client-threshold 925
config rogue detection min-rssi 926
config rogue detection monitor-ap 927
config rogue detection report-interval 929
config rogue detection security-level 930
config rogue detection transient-rogue-interval 931
config rogue rule 932
config rogue rule condition ap 937
config remote-lan session-timeout 939
config rfid auto-timeout 940
config rfid status 941
config rfid timeout 942
config rogue ap timeout 943
config route add 944
config route delete 945
config serial baudrate 946
config serial timeout 947
config service timestamps 948
config sessions maxsessions 949
config sessions timeout 950
config slot 951
config switchconfig boot-break 953
config switchconfig fips-prerequisite 954
config switchconfig ucapl 955
config switchconfig wlancc 956
config switchconfig strong-pwd 957
config switchconfig flowcontrol 960
config switchconfig mode 961
config switchconfig secret-obfuscation 962
config sysname 963
config snmp community accessmode 964
config snmp community create 965
config snmp community delete 966
config snmp community ipaddr 967

config snmp community mode 968
config snmp engineID 969
config snmp syscontact 970
config snmp syslocation 971
config snmp trapreceiver create 972
config snmp trapreceiver delete 973
config snmp trapreceiver mode 974
config snmp v3user create 975
config snmp v3user delete 977
config snmp version 978
config tacacs acct 979
config tacacs athr 981
config tacacs athr mgmt-server-timeout 983
config tacacs auth 984
config tacacs auth mgmt-server-timeout 986
config tacacs dns 987
config tacacs fallback-test interval 989
config time manual 990
config time ntp 991
config time timezone 994
config time timezone location 995
config trapflags 802.11-Security 999
config trapflags aaa 1000
config trapflags adjchannel-rogueap 1001
config trapflags ap 1002
config trapflags authentication 1003
config trapflags client 1004
config trapflags client max-warning-threshold 1006
config trapflags configsave 1007
config trapflags IPsec 1008
config trapflags linkmode 1010
config trapflags mesh 1011
config trapflags multiusers 1012
config trapflags rfid 1013

config trapflags rogueap 1015
config trapflags rrm-params 1016
config trapflags rrm-profile 1017
config trapflags stpmode 1018
config trapflags strong-pwdcheck 1019
config trapflags wps 1020
config tunnel eogre heart-beat 1021
config tunnel eogre gateway 1022
config tunnel eogre domain 1023
config tunnel profile 1024
config tunnel profile_rule 1025
config tunnel profile_rule-delete 1026
config tunnel profile eogre-DHCP82 1027
config tunnel profile eogre-gateway-radius-proxy 1028
config tunnel profile eogre-gateway-radius-proxy-accounting 1029
config tunnel profile eogre-DHCP82 1030
config tunnel profile eogre-DHCP82-circuit-id 1031
config tunnel profile eogre-DHCP82-delimiter 1032
config tunnel profile eogre-DHCP82-format 1033
config tunnel profile eogre-DHCP82-remote-id 1034
config watchlist add 1035
config watchlist delete 1036
config watchlist disable 1037
config watchlist enable 1038
config wgb vlan 1039
config wlan 1040
config wlan 7920-support 1042
config wlan 802.11e 1043
config wlan aaa-override 1044
config wlan acl 1046
config wlan apgroup 1047
config wlan apgroup atf 802.11 1056
config wlan apgroup atf 802.11 policy 1057
config wlan apgroup qinq 1058

config wlan assisted-roaming 1060
config wlan atf 1061
config wlan avc 1062
config wlan band-select allow 1063
config wlan broadcast-ssid 1064
config wlan call-snoop 1065
config wlan chd 1066
config wlan ccx aironet-ie 1067
config wlan channel-scan defer-priority 1068
config wlan channel-scan defer-time 1069
config wlan custom-web 1070
config wlan dhcp_server 1072
config wlan diag-channel 1073
config wlan dtim 1074
config wlan exclusionlist 1075
config wlan fabric 1076
config wlan flexconnect ap-auth 1077
config wlan flexconnect central-assoc 1078
config wlan flexconnect learn-ipaddr 1079
config wlan flexconnect local-switching 1080
config wlan flexconnect vlan-central-switching 1082
config wlan flow 1083
config wlan hotspot 1084
config wlan hotspot dot11u 1085
config wlan hotspot dot11u 3gpp-info 1086
config wlan hotspot dot11u auth-type 1087
config wlan hotspot dot11u disable 1088
config wlan hotspot dot11u domain 1089
config wlan hotspot dot11u enable 1090
config wlan hotspot dot11u hessid 1091
config wlan hotspot dot11u ipaddr-type 1092
config wlan hotspot dot11u nai-realm 1093
config wlan hotspot dot11u network-type 1096
config wlan hotspot dot11u roam-oi 1097

config wlan hotspot hs2 **1098**
config wlan hotspot hs2 domain-id **1101**
config wlan hotspot hs2 osu legacy-ssid **1102**
config wlan hotspot hs2 osu sp create **1103**
config wlan hotspot hs2 osu sp delete **1104**
config wlan hotspot hs2 osu sp icon-file add **1105**
config wlan hotspot hs2 osu sp icon-file delete **1106**
config wlan hotspot hs2 osu sp method add **1107**
config wlan hotspot hs2 osu sp method delete **1108**
config wlan hotspot hs2 osu sp nai add **1109**
config wlan hotspot hs2 osu sp nai delete **1110**
config wlan hotspot hs2 osu sp uri add **1111**
config wlan hotspot hs2 osu sp uri delete **1112**
config wlan hotspot hs2 wan-metrics downlink **1113**
config wlan hotspot hs2 wan-metrics link-status **1114**
config wlan hotspot hs2 wan-metrics lmd **1115**
config wlan hotspot hs2 wan-metrics uplink **1116**
config wlan hotspot msap **1117**
config wlan interface **1118**
config wlan ipv6 acl **1119**
config wlan kts-cac **1120**
config wlan layer2 acl **1121**
config wlan ldap **1122**
config wlan learn-ipaddr-cswlan **1123**
config wlan load-balance **1124**
config wlan mac-filtering **1125**
config wlan max-associated-clients **1126**
config wlan max-radio-clients **1127**
config wlan mdns **1128**
config wlan media-stream **1129**
config wlan mfp **1130**
config wlan mobility anchor **1131**
config wlan mobility foreign-map **1132**
config wlan multicast buffer **1133**

config wlan multicast interface 1134
config wlan mu-mimo 1135
config wlan nac 1136
config wlan override-rate-limit 1137
config wlan passive-client 1139
config wlan peer-blocking 1140
config wlan pmipv6 default-realm 1141
config wlan pmipv6 mobility-type 1142
config wlan pmipv6 profile_name 1143
config wlan policy 1144
config wlan profile 1145
config wlan profiling 1146
config wlan qos 1148
config wlan radio 1149
config wlan radius_server acct 1150
config wlan radius_server acct interim-update 1152
config wlan radius_server auth 1153
config wlan radius_server overwrite-interface 1154
config wlan radius_server realm 1155
config wlan roamed-voice-client re-anchor 1156
config wlan security 802.1X 1157
config wlan security ckip 1159
config wlan security cond-web-redir 1161
config wlan security eap-params 1162
config wlan security eap-passthru 1164
config wlan security ft 1165
config wlan security ft over-the-ds 1166
config wlan security IPsec disable 1167
config wlan security IPsec enable 1168
config wlan security IPsec authentication 1169
config wlan security IPsec encryption 1170
config wlan security IPsec config 1171
config wlan security IPsec ike authentication 1172
config wlan security IPsec ike dh-group 1173

config wlan security IPsec ike lifetime 1174
config wlan security IPsec ike phase1 1175
config wlan security IPsec ike contivity 1176
config wlan security wpa akm ft 1177
config wlan security ft 1178
config wlan security passthru 1179
config wlan security pmf 1180
config wlan security splash-page-web-redir 1182
config wlan security static-wep-key authentication 1183
config wlan security static-wep-key disable 1184
config wlan security static-wep-key enable 1185
config wlan security static-wep-key encryption 1186
config wlan security tkip 1187
config wlan usertimeout 1188
config wlan security web-auth 1189
config wlan security web-passthrough acl 1191
config wlan security web-passthrough disable 1192
config wlan security web-passthrough email-input 1193
config wlan security web-passthrough enable 1194
config wlan security wpa akm 802.1x 1195
config wlan security wpa akm cckm 1196
config wlan security wpa akm ft 1197
config wlan security wpa akm pmf 1198
config wlan security wpa akm psk 1199
config wlan security wpa disable 1200
config wlan security wpa enable 1201
config wlan security wpa ciphers 1202
config wlan security wpa gtk-random 1203
config wlan security wpa osen disable 1204
config wlan security wpa osen enable 1205
config wlan security wpa wpa1 disable 1206
config wlan security wpa wpa1 enable 1207
config wlan security wpa wpa2 disable 1208
config wlan security wpa wpa2 enable 1209

config wlan security wpa wpa2 cache 1210
config wlan security wpa wpa2 cache sticky 1211
config wlan security wpa wpa2 ciphers 1212
config wlan session-timeout 1213
config wlan sip-cac disassoc-client 1215
config wlan sip-cac send-486busy 1216
config wlan ssid 1217
config wlan static-ip tunneling 1218
config wlan uapsd compliant client enable 1219
config wlan uapsd compliant-client disable 1220
config wlan user-idle-threshold 1221
config wlan usertimeout 1222
config wlan webauth-exclude 1223
config wlan wifidirect 1224
config wlan wmm 1225
config wps ap-authentication 1226
config wps auto-immune 1227
config wps cids-sensor 1228
config wps client-exclusion 1230
config wps mfp 1232
config wps shun-list re-sync 1233
config wps signature 1234
config wps signature frequency 1236
config wps signature interval 1237
config wps signature mac-frequency 1238
config wps signature quiet-time 1239
config wps signature reset 1240

第 IV 部 : **debug コマンド** 1241

第 8 章 **debug コマンド : 802.11** 1243

debug 11k 1244
debug 11w-pmf 1245
debug 11v all 1246

debug 11v detail 1247
debug 11v error 1248
debug 11w-pmf 1249

第 9 章 **debug コマンド：a ～ i** 1251
debug aaa 1253
debug aaa events 1255
debug aaa local-auth 1256
debug airewave-director 1258
debug ap 1260
debug ap enable 1262
debug ap packet-dump 1263
debug ap show stats 1264
debug ap show stats video 1266
debug arp 1267
debug avc 1268
debug bcast 1269
debug call-control 1270
debug capwap 1271
debug capwap reap 1272
debug ccxdiag 1273
debug ccxrm 1274
debug ccxs69 1275
debug cckm 1276
debug client 1277
debug cts sxp 1278
debug cac 1279
debug cdp 1281
debug crypto 1282
debug dhcp 1283
debug dhcp service-port 1284
debug disable-all 1285
debug dns 1286
debug dot11 1287

debug dot11 1288
debug dot11 mgmt interface 1289
debug dot11 mgmt msg 1290
debug dot11 mgmt ssid 1291
debug dot11 mgmt state-machine 1292
debug dot11 mgmt station 1293
debug dot1x 1294
debug dtls 1295
debug fastpath 1296
debug flexconnect avc 1302
debug flexconnect aaa 1303
debug flexconnect acl 1304
debug flexconnect cckm 1305
debug group 1306
debug fmchs 1307
debug flexconnect client ap 1308
debug flexconnect client ap syslog 1309
debug flexconnect client group 1310
debug flexconnect client group syslog 1311
debug flexconnect group 1312
debug ft 1313
debug hotspot 1314
debug ipv6 1315

第 10 章 **debug コマンド：j ～ q** 1317
debug l2age 1318
debug mac 1319
debug mdns all 1320
debug mdns detail 1321
debug mdns error 1322
debug mdns message 1323
debug mdns ha 1324
debug memory 1325
debug mesh security 1326

debug mesh convergence 1327
debug mobility 1328
debug nac 1330
debug nmsp 1331
debug ntp 1332
debug packet error 1333
debug packet logging 1334
debug pem 1337
debug pm 1338
debug poe 1340
debug policy 1341
debug profiling 1342

第 11 章 **debug コマンド：r ～ z** 1343
debug rbcp 1344
debug rfid 1345
debug snmp 1346
debug transfer 1347
debug voice-diag 1348
debug wcp 1350
debug web-auth 1351
debug wips 1352
debug wps sig 1353
debug wps mfp 1354

第 V 部： **IMM コマンド** 1355

第 12 章 **IMM コマンド** 1357
imm address 1358
imm dhcp 1359
imm mode 1360
imm restart 1361
imm summary 1362
imm username 1363

第 VI 部 : **license コマンド** 1365

第 13 章 **license コマンド** 1367

license activate ap-count eval 1368
license activate feature 1369
license add ap-count 1370
license add feature 1371
license clear 1372
license comment 1373
license deactivate ap-count eval 1374
license deactivate feature 1375
license delete ap-count 1376
license delete feature 1377
license install 1378
license modify priority 1379
license revoke 1381
license save 1382
license smart 1383

第 VII 部 : **show コマンド** 1385

第 14 章 **show コマンド : 802.11** 1387

show 802.11 1388
show 802.11 1390
show 802.11 cleanair 1392
show 802.11 cleanair air-quality summary 1394
show 802.11 cleanair air-quality worst 1395
show 802.11 cleanair device ap 1396
show 802.11 cleanair device type 1397
show 802.11 cu-metrics 1399
show 802.11 extended 1400
show 802.11 media-stream 1402

第 15 章 **show コマンド：a ～ i** 1403

show aaa auth 1408
show acl 1409
show acl detailed 1411
show acl summary 1412
show advanced 802.11 channel 1413
show advanced 802.11 coverage 1414
show advanced 802.11 group 1415
show advanced 802.11 l2roam 1416
show advanced 802.11 logging 1417
show advanced 802.11 monitor 1418
show advanced 802.11 optimized roaming 1419
show advanced 802.11 profile 1420
show advanced 802.11 receiver 1421
show advanced 802.11 summary 1422
show advanced 802.11 txpower 1423
show advanced backup-controller 1424
show advanced dot11-padding 1425
show advanced hotspot 1426
show advanced max-1x-sessions 1427
show advanced probe 1428
show advanced rate 1429
show advanced timers 1430
show advanced client-handoff 1431
show advanced eap 1432
show advanced send-disassoc-on-handoff 1433
show advanced sip-preferred-call-no 1434
show advanced sip-snooping-ports 1435
show arp kernel 1436
show arp switch 1437
show ap auto-rf 1438
show ap aid-audit-mode 1440
show ap ccx rm 1441

show ap cdp 1442
show ap channel 1444
show ap config 1445
show ap config general 1451
show ap config global 1452
show ap core-dump 1453
show ap crash-file 1454
show ap data-plane 1455
show ap dtls-cipher-suite 1456
show ap ethernet tag 1457
show ap eventlog 1458
show ap flexconnect 1459
show ap image 1460
show ap inventory 1461
show ap join stats detailed 1462
show ap join stats summary 1463
show ap join stats summary all 1464
show ap led-state 1465
show ap led-flash 1466
show ap link-encryption 1467
show ap max-count summary 1468
show ap monitor-mode summary 1469
show ap module summary 1470
show ap packet-dump status 1471
show ap prefer-mode stats 1472
show ap retransmit 1473
show ap stats 1474
show ap summary 1477
show ap tcp-mss-adjust 1478
show ap wlan 1479
show assisted-roaming 1480
show atf config 1481
show atf statistics ap 1482
show auth-list 1483

show avc applications 1484
show avc engine 1485
show avc profile 1486
show avc protocol-pack 1487
show avc statistics application 1488
show avc statistics client 1490
show avc statistics guest-lan 1492
show avc statistics remote-lan 1494
show avc statistics top-apps 1496
show avc statistics wlan 1498
show boot 1500
show band-select 1501
show buffers 1502
show cac voice stats 1504
show cac voice summary 1505
show cac video stats 1506
show cac video summary 1508
show call-control ap 1509
show call-control client 1514
show call-home summary 1515
show capwap reap association 1516
show capwap reap status 1517
show cdp 1518
show certificate compatibility 1519
show certificate lsc 1520
show certificate ssc 1521
show certificate summary 1522
show client ap 1523
show client calls 1524
show client ccx client-capability 1525
show client ccx frame-data 1526
show client ccx last-response-status 1527
show client ccx last-test-status 1528
show client ccx log-response 1529

show client ccx manufacturer-info 1531
show client ccx operating-parameters 1532
show client ccx profiles 1533
show client ccx results 1535
show client ccx rm 1536
show client ccx stats-report 1538
show client detail 1539
show client location-calibration summary 1543
show client roam-history 1544
show client summary 1545
show client summary guest-lan 1547
show client tsm 1548
show client username 1550
show client voice-diag 1551
show client detail 1552
show client location-calibration summary 1554
show client probing 1555
show client roam-history 1556
show client summary 1557
show client wlan 1559
show cloud-services cmx summary 1560
show cloud-services cmx statistics 1561
show coredump summary 1562
show country 1563
show country channels 1564
show country supported 1565
show cpu 1567
show custom-web 1568
show database summary 1569
show dhcp 1570
show dhcp proxy 1571
show dhcp timeout 1572
show dtls connections 1573
show exclusionlist 1574

show flexconnect acl detailed 1575
show flexconnect acl summary 1576
show flexconnect group detail 1577
show flexconnect group summary 1578
show flexconnect office-extend 1579
show flow exporter 1580
show flow monitor summary 1581
show guest-lan 1582
show icons summary 1583
show ike 1584
show interface summary 1585
show interface detailed 1586
show interface group 1589
show invalid-config 1591
show inventory 1592
show IPsec 1593
show ipv6 acl 1595
show ipv6 summary 1596
show guest-lan 1597
show icons file-info 1598
show ipv6 acl 1599
show ipv6 acl cpu 1600
show ipv6 acl detailed 1601
show ipv6 neighbor-binding 1602
show ipv6 ra-guard 1606
show ipv6 route summary 1607
show ipv6 summary 1608
show known ap 1609

第 16 章 **show コマンド：j ～ q** 1611
show l2tp 1614
show lag eth-port-hash 1615
show lag ip-port-hash 1616
show lag summary 1617

show ldap 1618
show ldap statistics 1619
show ldap summary 1620
show license all 1621
show license capacity 1623
show license detail 1624
show license expiring 1625
show license evaluation 1626
show license feature 1627
show license file 1628
show license handle 1629
show license image-level 1630
show license in-use 1631
show license permanent 1632
show license status 1633
show license statistics 1634
show license summary 1635
show license udi 1637
show license usage 1638
show load-balancing 1639
show local-auth config 1640
show local-auth statistics 1642
show local-auth certificates 1644
show logging 1645
show logging config-history 1647
show logging flags 1648
show loginsession 1649
show macfilter 1650
show mdns ap summary 1651
show mdns domain-name-ip summary 1652
show mdns profile 1654
show mdns service 1656
show media-stream client 1658
show media-stream group detail 1659

show media-stream group summary 1660
show mesh ap 1661
show mesh astools stats 1663
show mesh backhaul 1664
show mesh cac 1665
show mesh client-access 1667
show mesh config 1668
show mesh convergence 1669
show mesh env 1670
show mesh neigh 1671
show mesh path 1674
show mesh per-stats 1675
show mesh public-safety 1676
show mesh queue-stats 1677
show mesh security-stats 1678
show mesh stats 1680
show mgmtuser 1681
show mobility anchor 1682
show mobility ap-list 1684
show mobility foreign-map 1685
show mobility group member 1686
show mobility oracle 1687
show mobility statistics 1689
show mobility summary 1690
show msglog 1692
show nac statistics 1693
show nac summary 1694
show network 1695
show network summary 1696
show netuser 1698
show netuser guest-roles 1699
show network multicast mgid detail 1700
show network multicast mgid summary 1701
show network summary 1702

show nmsp notify-interval summary 1704
show nmsp status 1705
show nmsp statistics 1706
show nmsp subscription 1708
show nmsp subscription summary 1710
show ntp-keys 1711
show ntp-keys 1712
show pmk-cache 1713
show pmipv6 domain 1714
show pmipv6 mag bindings 1715
show pmipv6 mag globals 1716
show pmipv6 mag stats 1717
show pmipv6 profile summary 1719
show policy 1720
show port 1722
show profiling policy summary 1724
show qos 1727
show qos qosmap 1728
show queue-info 1729

第 17 章 **show コマンド：r ～ z** 1731
show radius acct detailed 1734
show radius acct statistics 1735
show radius auth detailed 1736
show radius auth statistics 1737
show radius avp-list 1738
show radius summary 1739
show redundancy interfaces 1740
show redundancy latency 1741
show redundancy mobilitymac 1742
show redundancy peer-route summary 1743
show redundancy peer-system statistics 1744
show redundancy statistics 1745
show redundancy summary 1746

show redundancy timers 1747
show remote-lan 1748
show reset 1750
show rfid client 1751
show rfid config 1752
show rfid detail 1753
show rfid summary 1754
show rf-profile summary 1755
show rf-profile details 1756
show rogue adhoc custom summary 1757
show rogue adhoc detailed 1758
show rogue adhoc friendly summary 1760
show rogue adhoc malicious summary 1761
show rogue adhoc unclassified summary 1762
show rogue adhoc summary 1763
show rogue ap clients 1764
show rogue ap custom summary 1766
show rogue ap detailed 1768
show rogue ap friendly summary 1771
show rogue ap malicious summary 1773
show rogue ap summary 1775
show rogue ap unclassified summary 1778
show rogue auto-contain 1779
show rogue client detailed 1780
show rogue client summary 1781
show rogue ignore-list 1782
show rogue rule detailed 1784
show rogue rule summary 1786
show route kernel 1787
show route summary 1788
show rules 1789
show run-config 1790
show run-config startup-commands 1791
show serial 1792

show sessions 1793
show snmpcommunity 1794
show snmpengineID 1795
show snmptrap 1796
show snmpv3user 1797
show snmpversion 1798
show spanningtree port 1799
show spanningtree switch 1800
show stats port 1801
show stats switch 1803
show switchconfig 1805
show sysinfo 1806
show system iostat 1807
show system top 1808
show tacacs acct statistics 1812
show tacacs athr statistics 1813
show tacacs auth statistics 1814
show tacacs summary 1815
show tech-support 1816
show time 1817
show trapflags 1819
show traplog 1821
show tunnel profile-summary 1822
show tunnel profile-detail 1823
show tunnel eogre-summary 1824
show tunnel eogre-statistics 1825
show tunnel eogre-domain-summary 1826
show tunnel eogre gateway 1827
show watchlist 1828
show wlan 1829
show wps ap-authentication summary 1834
show wps cids-sensor 1835
show wps mfp 1836
show wps shun-list 1837

show wps signature detail 1838
show wps signature events 1839
show wps signature summary 1841
show wps summary 1843
show wps wips statistics 1845
show wps wips summary 1846
show wps ap-authentication summary 1847

第 VIII 部： その他のコマンド 1849

第 18 章 その他のコマンド：1 1851
cping 1852
eping 1853
mping 1854
ping 1855

第 19 章 その他のコマンド：1 1857
capwap ap controller ip address 1859
capwap ap dot1x 1860
capwap ap hostname 1861
capwap ap ip address 1862
capwap ap ip default-gateway 1863
capwap ap log-server 1864
capwap ap mode 1865
capwap ap primary-base 1866
capwap ap primed-timer 1867
capwap ap secondary-base 1868
capwap ap tertiary-base 1869
lwapp ap controller ip address 1870
reset system at 1871
reset system in 1872
reset system cancel 1873
reset system notify-time 1874
reset peer-system 1875

save config 1876
transfer download certpasswor 1877
transfer download datatype 1878
transfer download datatype icon 1880
transfer download filename 1881
transfer download mode 1882
transfer download password 1883
transfer download path 1884
transfer download port 1885
transfer download serverip 1886
transfer download start 1887
transfer download tftpPktTimeout 1888
transfer download tftpMaxRetries 1889
transfer download username 1890
transfer encrypt 1891
transfer upload datatype 1892
transfer upload filename 1894
transfer upload mode 1895
transfer upload pac 1896
transfer upload password 1897
transfer upload path 1898
transfer upload peer-start 1899
transfer upload port 1900
transfer upload serverip 1901
transfer upload start 1902
transfer upload username 1903

第 IX 部 : **Mobility Express コントローラ コマンド** 1905

第 20 章 **Mobility Express コントローラ コマンド** 1907

アプリケーションの可視性コマンド 1908
ログ、コア、およびクラッシュ ファイルを収集するためのコマンド 1909
Cisco.com からソフトウェアをダウンロードするためのコマンド 1910

CleanAir コマンド 1911
CMX クラウド コマンド 1912
コントローラ イメージのアップグレード コマンド 1913
DNS コマンド 1914
移行コマンド 1915
NTP コマンド 1916
次の優先マスター AP と強制フェールオーバー 1917
UX 規制ドメイン コマンド 1918
VRRP コマンド 1919
WGB コマンド 1920
WLAN のセキュリティ コマンド 1921

はじめに

ここでは、『に記載されているAireOSコマンドのみをサポートしています。また、他のマニュアルの入手方法についても説明します。この章は、次の項で構成されています。

- 対象読者 （li ページ）
- 表記法 （li ページ）
- 関連資料 （liv ページ）
- マニュアルの入手方法およびテクニカル サポート （liv ページ）

対象読者

このマニュアルは、シスコ ワイヤレス コントローラ（Cisco WLC）およびCisco Lightweight アクセスポイント（CiscoAP）を設定および管理する経験豊富なネットワーク管理者を対象とします。

（注） **test** コマンドを使用すると、Cisco WLC の予期しない再起動など、システムが中断することがあります。このため、デバッグ目的で**test** コマンドをCisco WLC で使用する際はCisco Technical Assistance Center（TAC）担当者の支援を受けることをお勧めします。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。

表記法	説明
{x | y | z }	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。（このマニュアルに記載されている警告の翻訳を参照するには、付録の「翻訳版の安全上の警告」を参照してください）。

警告タイトル	説明
Waarschuwing	Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)
Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").

警告タイトル	説明
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

関連資料

Cisco ソリューションについては、併せて次のマニュアルも参照してください。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

『What's New in Cisco Product Documentation』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 I 部

コマンドライン インターフェイスの使用

- コマンドライン インターフェイスの使用 （1 ページ）

コマンドライン インターフェイスの使用

この章は、次の内容で構成されています。

- CLI コマンドのキーボード ショートカット （2 ページ）
- 対話型ヘルプ機能の使用 （4 ページ）

CLI コマンドのキーボード ショートカット

次の表には、コントローラのコマンドラインを入力し、編集するのに役立つ CLI キーボード ショートカットを示します。

表 *1: CLI* コマンドのキーボード ショートカット

アクション	説明	キーボードのショートカット
変更	カーソルの位置にある単語を小文字に変更します。	Esc+I
	カーソルの位置にある単語を大文字に変更します。	Esc+u
削除	カーソルの左にある文字。	Ctrl+h、Delete、または Back Space キー
	カーソル位置から行の先頭までのすべての文字。	Ctrl+u
	カーソル位置から行の末尾までのすべての文字。	Ctrl+k
	カーソル位置から単語の末尾までのすべての文字。	Esc+d
	カーソル位置の左の単語。	Ctrl+w または Esc Backspace
詳細な出力を表示します。	詳細出力を終了します。	q、Q、または Ctrl+C
	次の追加画面。デフォルトは 1 画面です。複数の画面を表示するには、Space キーを押す前に番号を入力します。	Space
	次の行。デフォルトは 1 行です。複数の行を表示するには、Enter キーを押す前に番号を入力します。	Enter
Enter または Return キー文字。		Ctrl+m
コマンドまたは省略形を展開します。		Ctrl+t または Tab キー
カーソルを移動します。	左（後ろ）に 1 文字。	Ctrl+b または左矢印キー
	右（前）に 1 文字。	Ctrl+f または右矢印キー

アクション	説明	キーボードのショートカット
	現在の単語または以前に入力した単語の先頭まで、左（後ろ）に 1 単語。	Esc+b
	現在の単語または次の単語の末尾まで、右（前）に 1 単語。	Esc+f
	コマンドラインの先頭へ移動します。	Ctrl+a
	行の末尾。	Ctrl+e
プロンプトで画面を再描画します。		Ctrl+l または Ctrl+r
任意の設定モードから EXEC モードに戻ります。		Ctrl-z
前のモードに戻るか、または EXEC モードから CLI を終了します。		exit コマンド
カーソルの左にある文字を、カーソル位置の文字と置き換えます。		Ctrl+t

対話型ヘルプ機能の使用

疑問符（?）文字を入力すると、コマンドラインにコマンドについて、次の種類のヘルプが表示されます。次の表に、対話型ヘルプ機能のリストを示します。

表 *2:* 対話型ヘルプ機能のリスト

コマンド	説明
help	任意のコマンド モードでヘルプ機能を簡単に説明します。
コマンド プロンプトで ? を入力	特定のコマンド モードで使用可能なすべてのコマンドをリストします。
コマンドの一部?	文字列で始まるコマンドの一覧を表示します。
コマンドの一部<Tab>	特定のコマンド名を補完します。
コマンド ?	コマンドに関連付けられたキーワード、引数、またはその両方を示します。
コマンド キーワード ?	キーワードに関連する引数の一覧を表示します。

help コマンドの使用方法

始める前に

キーボード コマンドを検索するには、ルート レベルで help コマンドを使用します。

help

ヘルプは、疑問符「?」を入力することによって、コマンドの任意の位置で、要求できます。一致する項目がない場合、ヘルプ リストは空になります。? を入力して利用できるオプションが表示されるまで、後ろに戻る必要があります。次の 2 つのタイプのヘルプを使用できます。

1. コマンド引数を入力する準備ができているときに、詳細なヘルプを利用でき、使用できる各引数が説明されます。
2. 引数の一部を入力し、入力した引数と一致する引数を知りたいときに、部分的なヘルプが提供されます（show pr? など）。

例：

```
> help
HELP:
Special keys:
  DEL, BS... delete previous character
```

```
Ctrl-A  .... go to beginning of line
Ctrl-E  .... go to end of line
Ctrl-F  .... go forward one character
Ctrl-B  .... go backward one character
Ctrl-D  .... delete current character
Ctrl-U, X. delete to beginning of line
Ctrl-K  .... delete to end of line
Ctrl-W  .... delete previous word
Ctrl-T  .... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer
Ctrl-Z  .... return to root command prompt
Tab, <SPACE> command-line completion
Exit    .... go to next lower command prompt
?       .... list choices
```

? コマンドの使用方法

始める前に

コマンド ツリーの現在レベルのコマンドすべてや、特定のコマンドの詳細情報を表示するには、? コマンドを使用します。

コマンド名 **?**

コマンド情報の要求を入力するときには、**command name** と **?** の間にスペースを入れてください。

例

このコマンドは、ルート レベルから使用可能なすべてのコマンドとレベルを示します。

```
> ?
clear          Clear selected configuration elements.
config         Configure switch options and settings.
debug          Manages system debug options.
help           Help
linktest       Perform a link test to a specified MAC address.
logout         Exit this session. Any unsaved changes are lost.
ping           Send ICMP echo packets to a specified IP address.
reset          Reset options.
save           Save switch configurations.
show           Display switch options and settings.
transfer       Transfer a file to or from the switch.
```

コマンドの一部と ? の使用法

始める前に

文字列で始まるコマンドの一覧を表示するには、コマンドの一部と ? を使用します。

partial command?

コマンドと疑問符の間にスペースは使用できません。

次に、文字列「ad」で始まるコマンドを出力する例を示します。

```
> controller> config>ad?
```

文字列「ad」と一致するコマンドは、次のとおりです。

```
advanced
```

コマンド名の一部と <tab> の使用法

始める前に

途中まで入力したコマンド名をすべて入力するには、コマンドの一部と <tab> を使用します。

partial command<tab>

コマンドと <tab> 間にスペースは使用できません。

次に、途中まで入力した文字列「cert」で始まるコマンド名をすべて入力する例を示します。

```
Controller >config>cert<tab> certificate
```

コマンドと ? の使用法

例

コマンドに関連するキーワード、引数、または両方を一覧表示するには、コマンドと ? を使用します。

command-name ?

コマンドと疑問符の間にスペースが必要です。

次に、acl コマンドの引数およびキーワードをリストする例を示します。

```
Controller >config acl ?
```

以下に類似した情報が表示されます。

```
apply          Applies the ACL to the data path.
counter        Start/Stop the ACL Counters.
create         Create a new ACL.
delete         Delete an ACL.
rule           Configure rules in the ACL.
cpu            Configure the CPU ACL Information
```

コマンド キーワード?

キーワードに関連する引数の一覧を表示するには、コマンド キーワードと ? を使用します。

command keyword ?

キーワードと疑問符の間にスペースが必要です。

次に、キーワード cpu に関連する引数を表示する例を示します。

```
Controller >config acl cpu ?
```

以下に類似した情報が表示されます。

```
none            None - Disable the CPU ACL
<name>          <name> - Name of the CPU ACL
```

第 II 部

clear コマンド

- clear コマンド：a ～ l （11 ページ）
- clear コマンド：m ～ z （31 ページ）

clear コマンド：a ～ l

- clear advanced （12 ページ）
- clear acl counters （13 ページ）
- clear ap config （14 ページ）
- clear ap eventlog （15 ページ）
- clear ap join stats （16 ページ）
- clear arp （17 ページ）
- clear ap tsm （18 ページ）
- clear atf （19 ページ）
- clear avc statistics （20 ページ）
- clear client tsm （22 ページ）
- clear config （23 ページ）
- clear ext-webauth-url （24 ページ）
- clear location rfid （25 ページ）
- clear location statistics rfid （26 ページ）
- clear locp statistics （27 ページ）
- clear login-banner （28 ページ）
- clear lwapp private-config （29 ページ）

clear advanced

EDCAパラメータ、パケットパラメータ、または最適化ローミング統計情報をデフォルト値にリセットするには、**clear advanced** コマンドを使用します。

clear advanced {**802.11a** | **802.11b**} {**optimized-roaming stats | packet | edca-parameter** }

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
optimized-roaming stats	802.11a最適化ローミング統計情報をクリックします。
パケット	802.11a パケット パラメータ設定をクリアします。
edca-parameter	802.11a EDCA パラメータ設定をクリックします。

コマンド デフォルト

なし

次に、EDCA パラメータ値をデフォルトにリセットする例を示します。

```
(Cisco Controller) >clear advanced 802.11a optimized-roaming stats

(Cisco Controller) >clear advanced 802.11a packet

(Cisco Controller) >clear advanced 802.11a edca-parameter
```

clear acl counters

アクセス コントロール リスト（ACL）の現在のカウンタをクリアするには、**clear acl counters** コマンドを使用します。

clear acl counters *acl_name*

構文の説明

acl_name	ACL 名です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ACL コントローラは、Cisco 4400 Series Controller、Cisco WiSM、および Catalyst 3750G Integrated Wireless LAN Controller Switch の各コントローラ上でのみ使用できます。

次に、acl1 の現在のカウンタをクリアする例を示します。

```
(Cisco Controller) >clear acl counters acl1
```

clear ap config

Lightweight アクセス ポイントの設定をクリア（デフォルト値にリセット）するには、**clear ap config** コマンドを使用します。

clear ap config *ap_name*

構文の説明

ap_name	アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

このコマンドを入力しても、アクセス ポイントの固定 IP アドレスはクリアされません。

次に ap1240_322115 という名前のアクセス ポイント用のアクセス ポイントの設定をクリアする例を示します。

```
(Cisco Controller) >clear ap config ap1240_322115
Clear ap-config will clear ap config and reboot the AP. Are you sure you want continue?
 (y/n)
```

clear ap eventlog

既存のイベント ログを削除し、コントローラに結合されている特定のアクセス ポイントまたはすべてのアクセス ポイント用に空のイベント ログ ファイルを作成するには、**clear ap eventlog** コマンドを使用します。

clear ap eventlog {**specific** *ap_name* | **all**}

構文の説明

specific	特定のアクセス ポイント ログ ファイルを指定します。
ap_name	イベント ログ ファイルが空にされるアクセス ポイントの名前。
all	コントローラに接続されているすべてのアクセス ポイントのイベント ログを削除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのアクセス ポイントのイベント ログを削除する例を示します。

```
(Cisco Controller) >clear ap eventlog all
This will clear event log contents for all APs. Do you want continue? (y/n) :y
All AP event log contents have been successfully cleared.
```

clear ap join stats

すべてのアクセス ポイントまたは特定のアクセス ポイントの参加統計情報をクリアするには、**clear ap join stats** コマンドを使用します。

clear ap join stats {**all** | *ap_mac*}

構文の説明

all	すべてのアクセス ポイントを指定します。
ap_mac	アクセス ポイントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのアクセス ポイントの参加統計情報をクリアする例を示します。

```
(Cisco Controller) >clear ap join stats all
```

clear arp

Address Resolution Protocol（ARP）テーブルをクリアするには、**clear arp** コマンドを使用します。

clear arp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ARP テーブルを消去する例を示します。

```
(Cisco Controller) >clear arp
Are you sure you want to clear the ARP cache? (y/n)
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear ap tsm

アクセス ポイントにアソシエートされたクライアントのトラフィック ストリーム メトリック（TSM）統計情報をクリアするには、**clear ap tsm** コマンドを使用します。

clear ap tsm {**802.11a** | **802.11b**} *cisco_ap* **all**

構文の説明

802.11a	アクセス ポイントにアソシエートされたクライアントの 802.11a TSM 統計情報をクリアします。
802.11b	アクセス ポイントにアソシエートされたクライアントの 802.11b TSM 統計情報をクリアします。
cisco_ap	Cisco Lightweight アクセス ポイント。
all	アクセス ポイントにアソシエートされたクライアントの TSM 統計情報をクリアします。

コマンド デフォルト

なし

次に、アクセス ポイントのすべてのクライアントに対する 802.11a TSM 統計情報をクリアする例を示します。

```
(Cisco Controller) >clear ap tsm 802.11a AP3600_1 all
```

clear atf

Cisco Air Time Fairness の設定または統計情報をクリアするには、**clear atf** コマンドを使用します。

clear atf {**config** | **statistics**}

構文の説明

config	Cisco ATF の設定をクリアします。
statistics	Cisco ATF の統計情報をクリアします。

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

次に、**clear atf config** コマンドの出力例を示します。

```
(Cisco Controller) >clear atf config
```

clear avc statistics

クライアントの Application Visibility and Control（AVC）統計情報、ゲスト LAN、リモート LAN、または WLAN をクリアするには、**clear avc statistics** コマンドを使用します。

clear avc statistics {**client** {**all** | *client-mac*} | **guest-lan** {**all** | *guest-lan-id*} | **remote-lan** {**all** | *remote-lan-id*} | **wlan** {**all** | *wlan-id*}}

構文の説明

client	クライアント AVC 統計情報をクリアします。
all	すべてのクライアント AVC 統計情報をクリアします。
client-mac	クライアントの MAC アドレス。
guest-lan	ゲスト LAN の AVC 統計情報をクリアします。
all	すべてのゲスト LAN の AVC 統計情報をクリアします。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子。
remote-lan	リモート LAN の AVC 統計情報をクリアします。
all	すべてのリモート LAN の AVC 統計情報をクリアします。
remote-lan-id	1 ～ 512 のリモート LAN 識別子。
wlan	WLAN の AVC 統計情報をクリアします。
all	すべての WLAN の AVC 統計情報をクリアします。
wlan-id	1 ～ 512 の WLAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントの AVC 統計情報をクリアする例を示します。

```
(Cisco Controller) >clear avc statistics client 00:21:1b:ea:36:60
```

関連コマンド

config avc profile create

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug avc error

debug avc events

clear client tsm

このクライアントがアソシエートされた特定のアクセス ポイントまたはすべてのアクセス ポイントのトラフィック ストリーム メトリック（TSM）統計情報をクリアするには、**clear client tsm** コマンドを使用します。

clear client tsm {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**}

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
client_mac	クライアントの MAC アドレス。
ap_mac	Cisco Lightweight アクセス ポイントの MAC アドレス。
all	すべてのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレスが 00:40:96:a8:f7:98 の TSM をクリアする例を示します。

```
(Cisco Controller) >clear client tsm 802.11a 00:40:96:a8:f7:98 all
```

関連コマンド

clear upload start

clear config

設定データを工場出荷時のデフォルト設定にリセットするには、**clear config** コマンドを使用します。

clear config

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、工場出荷時のデフォルトに設定データをリセットする例を示します。

```
(Cisco Controller) >clear config
Are you sure you want to clear the configuration? (y/n)
n
Configuration not cleared!
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear ext-webauth-url

外部 Web 認証の URL をクリアするには、**clear ext-webauth-url** コマンドを使用します。

clear ext-webauth-url

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、外部 Web 認証 URL をクリアする例を示します。

```
(Cisco Controller) >clear ext-webauth-url
URL cleared.
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear location rfid

データベース全体から、特定の無線周波数 ID（RFID）タグまたはすべての RFID タグをクリアするには、**clear location rfid** コマンドを使用します。

clear location rfid {*mac_address* | **all**}

構文の説明

mac_address	特定の RFID タグの MAC アドレス。
all	データベース上のすべての RFID タグを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、データベース上のすべての RFID タグをクリアする例を示します。

```
(Cisco Controller) >clear location rfid all
```

関連コマンド

clear location statistics rfid

config location

show location

show location statistics rfid

clear location statistics rfid

無線周波数 ID（RFID）の統計情報をクリアするには、**clear location statistics rfid** コマンドを使用します。

clear location statistics rfid

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RFID の統計情報をクリアする例を示します。

```
(Cisco Controller) >clear location statistics rfid
```

関連コマンド

config location

show location

show location statistics rfid

clear locp statistics

ロケーション プロトコル（LOCP）統計情報をクリアするには、**clear locp statistics** コマンドを使用します。

clear locp statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LOCP に関連する統計情報をクリアする例を示します。

```
(Cisco Controller) >clear locp statistics
```

関連コマンド

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp notify-interval summary

show nmsp statistics

show nmsp status

clear login-banner

コントローラからログイン バナー ファイルを削除するには、**clear login-banner** コマンドを使用します。

clear login-banner

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ログイン バナー ファイルをクリアする例を示します。

```
(Cisco Controller) >clear login-banner
```

関連コマンド

transfer download datatype

clear lwapp private-config

スタティック IP アドレスとコントローラ IP アドレス設定を含むアクセス ポイントの現在の Lightweight アクセス ポイント プロトコル（LWAPP）プライベート設定をクリア（デフォルト値にリセット）するには、**clear lwapp private-config** コマンドを使用します。

clear lwapp private-config

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

アクセス ポイントのコンソール ポートにコマンドを入力します。

アクセス ポイントのコンソール ポートを使用してアクセス ポイントの FlexConnect 設定を変更する前に、アクセス ポイントをスタンドアロン モード（Cisco WLC に接続されていない状態）にし、**clear lwapp private-config** コマンドを使用して現在の LWAPP プライベート設定を削除する必要があります。

（注） アクセス ポイントで Cisco Access Point IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、アクセス ポイントの現在の LWAPP プライベート設定をクリアする例を示します。

```
ap_console >clear lwapp private-config
removing the reap config file flash:/lwapp_reap.cfg
```

clear コマンド：m ～ z

- clear mdns service-database （32 ページ）
- clear nmsp statistics （33 ページ）
- clear radius acct statistics （34 ページ）
- clear session （35 ページ）
- clear tacacs auth statistics （36 ページ）
- clear redirect-url （37 ページ）
- clear stats ap wlan （38 ページ）
- clear stats local-auth （39 ページ）
- clear stats mobility （40 ページ）
- clear stats port （41 ページ）
- clear stats radius （42 ページ）
- clear stats smart-lic （44 ページ）
- clear stats switch （45 ページ）
- clear stats tacacs （46 ページ）
- clear transfer （47 ページ）
- clear traplog （48 ページ）
- clear webimage （49 ページ）
- clear webmessage （50 ページ）
- clear webtitle （51 ページ）

clear mdns service-database

マルチキャスト DNS サービス データベースをクリアするには、**clear mdns service-database** コマンドを使用します。

clear mdns service-database {**all** | *service-name*}

構文の説明

all	mDNS サービス データベースをクリアします。
service-name	mDNS サービスの名前。Cisco WLC は mDNS サービスの詳細をクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco WLC は、マスター サービス データベースで mDNS サービスが利用できる場合にのみ、このサービスのアドバタイズメントをスヌーピングおよび学習します。

次に mDNS サービス データベースをクリアする例を示します。

```
(Cisco Controller) >clear mdns service-database all
```

関連コマンド

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

config mdns profile

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

clear nmsp statistics

ネットワーク モビリティ サービス プロトコル（NMSP）の統計情報をクリアするには、**clear nmsp statistics** コマンドを使用します。

clear nmsp statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、NMSP 統計情報ログ ファイルを削除する例を示します。

```
(Cisco Controller) >clear nmsp statistics
```

関連コマンド

clear locp statistics

config nmsp notify-interval measurement

show nmsp notify-interval summary

show nmsp status

clear radius acct statistics

コントローラで RADIUS アカウンティングの統計情報をクリアするには、**clear radius acc statistics** コマンドを使用します。

clear radius acct statistics［**index** | **all**］

構文の説明

index	（任意）RADIUS アカウンティング サーバのインデックスを指定します。
all	（任意）すべての RADIUS アカウンティング サーバを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS アカウンティング統計情報をクリアする例を示します。

```
(Cisco Controller) >clear radius acc statistics
```

関連コマンド

show radius acct statistics

clear session

ユーザが Telnet または SSH を介してログインするときに作成されるセッションをクリアするには、**clear session** コマンドを使用します。

clear session *session-id*

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

セッションをクリアするためのセッション ID は、**show login-session** コマンドから取得される必要があります。

次に、Telnet または SSH セッションをクリアする例を示します。

```
(Cisco Controller) >clear session 3
```

clear tacacs auth statistics

コントローラで RADIUS 認証サーバ統計情報をクリアするには、**clear tacacs auth statistics** コマンドを使用します。

clear tacacs auth statistics［**index** | **all**］

構文の説明

index	（任意）RADIUS 認証サーバのインデックスを指定します。
all	（任意）すべての RADIUS 認証サーバを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバの統計情報をクリアする例を示します。

```
(Cisco Controller) >clear tacacs auth statistics
```

関連コマンド

show tacacs auth statistics

show tacacs summary

config tacacs auth

clear redirect-url

Cisco ワイヤレス LAN コントローラでカスタム Web 認証のリダイレクト用 URL をクリアするには、**clear redirect-url** コマンドを使用します。

clear redirect-url

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、カスタム Web 認証のリダイレクト用 URL をクリアする例を示します。

```
(Cisco Controller) >clear redirect-url
URL cleared.
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats ap wlan

WLAN の統計情報をクリアするには、**clear stats ap wlan** コマンドを使用します。

clear stats ap wlan *cisco_ap*

構文の説明

cisco_ap	選択した構成要素。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイント cisco_ap の WLAN 設定要素をクリアする例を示します。

```
(Cisco Controller) >clear stats ap wlan cisco_ap
WLAN statistics cleared.
```

clear stats local-auth

ローカルの拡張認証プロトコル（EAP）統計情報をクリアするには、**clear stats local-auth** コマンドを使用します。

clear stats local-auth

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ローカルの EAP 統計情報をクリアする例を示します。

```
(Cisco Controller) >clear stats local-auth
Local EAP Authentication Stats Cleared.
```

関連コマンド

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

clear stats mobility

Mobility Manager の統計情報をクリアするには、**clear stats mobility** コマンドを使用します。

clear stats mobility

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Mobility Manager の統計情報をクリアする例を示します。

```
(Cisco Controller) >clear stats mobility

   Mobility stats cleared.
```

clear stats port

特定のポートの統計カウンタをクリアするには、**clear stats port** コマンドを使用します。

clear stats port *port*

構文の説明

port	物理インターフェイスのポート番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ポート 9 の統計情報カウンタをクリアする例を示します。

```
(Cisco Controller) >clear stats port 9
```

関連コマンド

clear transfer
clear download datatype
clear download datatype
clear download filename
clear download mode
clear download serverip
clear download start
clear upload datatype
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start
clear stats port

clear stats radius

1 つ以上の RADIUS サーバの統計情報をクリアするには、**clear stats radius** コマンドを使用します。

clear stats radius {**auth** | **acct**} {**index** | **all**}

構文の説明

auth	認証に関する統計情報をクリアします。
acct	アカウンティングに関する統計情報をクリアします。
index	クリアする RADIUS サーバのインデックス番号を指定します。
all	すべての RADIUS サーバの統計情報をクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての RADIUS 認証サーバの統計情報をクリアする例を示します。

```
(Cisco Controller) >clear stats radius auth all
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear stats smart-lic

シスコ スマート ソフトウェアのすべての統計情報をクリアするには、**clear stats smart-lic** コマンドを使用します。

clear stats smart-lic

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、スマート ライセンスの統計情報をクリアする例を示します。

```
(Cisco Controller) >clear stats smart-lic

Initiated Smart Licensing statistics clear
```

clear stats switch

Cisco ワイヤレス LAN コントローラのすべてのスイッチ統計情報カウンタをクリアするには、**clear stats switch** コマンドを使用します。

clear stats switch

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのスイッチ統計カウンタをクリアする例を示します。

```
(Cisco Controller) >clear stats switch
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats tacacs

コントローラで TACACS+ サーバの統計情報をクリアするには、**clear stats tacacs** コマンドを使用します。

clear stats tacacs［**auth** | **athr** | **acct**］［**index** | **all**］

構文の説明

auth	（任意）TACACS+認証サーバの統計情報をクリアします。
athr	（任意）TACACS+許可サーバの統計情報をクリアします。
acct	（任意）TACACS+ アカウンティング サーバの統計情報をクリアします。
index	（任意）TACACS+サーバのインデックスを指定します。
all	（任意）すべての TACACS+ サーバを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、インデックス 1 の TACACS+ アカウンティング サーバの統計情報をクリアする例を示します。

```
(Cisco Controller) >clear stats tacacs acct 1
```

関連コマンド

show tacacs summary

clear transfer

転送情報をクリアするには、**clear transfer** コマンドを使用します。

clear transfer

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、転送情報をクリアする例を示します。

```
(Cisco Controller) >clear transfer
Are you sure you want to clear the transfer information? (y/n) y
Transfer Information Cleared.
```

関連コマンド

transfer upload datatype

transfer upload pac

transfer upload password

transfer upload port

transfer upload path

transfer upload username

transfer upload datatype

transfer upload serverip

transfer upload start

clear traplog

トラップ ログをクリアするには、**clear traplog** コマンドを使用します。

clear traplog

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、トラップ ログをクリアする例を示します。

```
(Cisco Controller) >clear traplog
Are you sure you want to clear the trap log? (y/n) y
Trap Log Cleared.
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear webimage

カスタム Web 認証のイメージをクリアするには、**clear webimage** コマンドを使用します。

clear webimage

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、カスタム Web 認証イメージをクリアする例を示します。

```
(Cisco Controller) >clear webimage
```

関連コマンド

clear transfer
clear download datatype
clear download filename
clear download mode
clear download path
clear download serverip
clear download start
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start

clear webmessage

カスタム Web 認証のメッセージをクリアするには、**clear webmessage** コマンドを使用します。

clear webmessage

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、カスタム Web 認証のメッセージをクリアする例を示します。

```
(Cisco Controller) >clear webmessage
Message cleared.
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear webtitle

カスタム Web 認証のタイトルをクリアするには、**clear webtitle** コマンドを使用します。

clear webtitle

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、カスタム Web 認証のタイトルをクリアする例を示します。

```
(Cisco Controller) >clear webtitle
Title cleared.
```

関連コマンド

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

第 III 部

コンフィギュレーション コマンド

- config コマンド：802.11 （55 ページ）
- config コマンド：a ～ i （175 ページ）
- config コマンド：j ～ q （543 ページ）
- config コマンド：r ～ z （797 ページ）

config コマンド：802.11

- config 802.11-abgn （58 ページ）
- config 802.11a 11acsupport （59 ページ）
- config 802.11-a antenna extAntGain （60 ページ）
- config 802.11-a channel ap （61 ページ）
- config 802.11-a txpower ap （62 ページ）
- config 802.11 antenna diversity （63 ページ）
- config 802.11 antenna extAntGain （64 ページ）
- config 802.11 antenna mode （65 ページ）
- config 802.11 antenna selection （66 ページ）
- config 802.11b 11gSupport （67 ページ）
- config 802.11b preamble （68 ページ）
- config 802.11h channelswitch （69 ページ）
- config 802.11h powerconstraint （70 ページ）
- config 802.11h setchannel （71 ページ）
- config 802.11 11nsupport （72 ページ）
- config 802.11 11nsupport a-mpdu tx priority （73 ページ）
- config 802.11 11nsupport a-mpdu tx scheduler （75 ページ）
- config 802.11 11nsupport antenna （76 ページ）
- config 802.11 11nsupport guard-interval （77 ページ）
- config 802.11 11nsupport mcs tx （78 ページ）
- config 802.11 11nsupport rifs （80 ページ）
- config 802.11 antenna diversity （81 ページ）
- config 802.11 antenna extAntGain （82 ページ）
- config 802.11 antenna mode （83 ページ）
- config 802.11 antenna selection （84 ページ）
- config 802.11 channel （85 ページ）
- config 802.11 channel ap （87 ページ）
- config 802.11 chan_width （88 ページ）
- config 802.11 rx-sop threshold （90 ページ）

- config 802.11 txPower （92 ページ）
- config 802.11 beamforming （94 ページ）
- config 802.11h channelswitch （96 ページ）
- config 802.11h powerconstraint （97 ページ）
- config 802.11h setchannel （98 ページ）
- config 802.11h smart dfs （99 ページ）
- config 802.11 11nsupport （100 ページ）
- config 802.11 11nsupport a-mpdu tx priority （101 ページ）
- config 802.11 11nsupport a-mpdu tx scheduler （103 ページ）
- config 802.11 11nsupport antenna （104 ページ）
- config 802.11 11nsupport guard-interval （105 ページ）
- config 802.11 11nsupport mcs tx （106 ページ）
- config 802.11 11nsupport rifs （108 ページ）
- config 802.11 beacon period （109 ページ）
- config 802.11 cac defaults （110 ページ）
- config 802.11 cac video acm （112 ページ）
- config 802.11 cac video cac-method （114 ページ）
- config 802.11 cac video load-based （116 ページ）
- config 802.11 cac video max-bandwidth （118 ページ）
- config 802.11 cac media-stream （120 ページ）
- config 802.11 cac multimedia （122 ページ）
- config 802.11 cac video roam-bandwidth （124 ページ）
- config 802.11 cac video sip （126 ページ）
- config 802.11 cac video tspec-inactivity-timeout （128 ページ）
- config 802.11 cac voice acm （130 ページ）
- config 802.11 cac voice max-bandwidth （132 ページ）
- config 802.11 cac voice roam-bandwidth （134 ページ）
- config 802.11 cac voice tspec-inactivity-timeout （136 ページ）
- config 802.11 cac voice load-based （138 ページ）
- config 802.11 cac voice max-calls （140 ページ）
- config 802.11 cac voice sip bandwidth （142 ページ）
- config 802.11 cac voice sip codec （144 ページ）
- config 802.11 cac voice stream-size （146 ページ）
- config 802.11 cleanair （148 ページ）
- config 802.11 cleanair device （151 ページ）
- config 802.11 cleanair alarm （153 ページ）
- config 802.11 disable （155 ページ）
- config 802.11 dtpc （156 ページ）
- config 802.11 enable （157 ページ）
- config 802.11 exp-bwreq （159 ページ）
- config 802.11 fragmentation （160 ページ）

- config 802.11 l2roam rf-params （161 ページ）
- config 802.11 max-clients （164 ページ）
- config 802.11 media-stream multicast-direct （165 ページ）
- config 802.11 media-stream video-redirect （167 ページ）
- config 802.11 multicast data-rate （168 ページ）
- config 802.11 rate （169 ページ）
- config 802.11 rssi-check （171 ページ）
- config 802.11 rssi-threshold （172 ページ）
- config 802.11 tsm （173 ページ）
- config 802.11b preamble （174 ページ）

config 802.11-abgn

アクセス ポイントのデュアル バンド無線パラメータを設定するには、**config 802.11-abgn** コマンドを使用します。

config 802.11-abgn {**cleanair** {**enable** | **disable**} {*cisco_ap* **band** *band*} | {**enable** | **disable**} {*cisco_ap*}}

構文の説明

cleanair	デュアル バンド無線に CleanAir を設定します。
enable	2.4 GHz と 5 GHz の両方の無線で CleanAir を有効にします。
disable	2.4 GHz と 5 GHz の両方の無線で CleanAir を無効にします。
cisco_ap	このコマンドを適用するアクセス ポイントの名前。
band	無線帯域を設定します。
band	2.4 GHz または 5 GHz となる無線帯域。
enable	アクセス ポイントのデュアル バンド無線を有効にします。
disable	アクセス ポイントのデュアル バンド無線を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco CleanAir 対応のアクセス ポイント無線のみが Cisco CleanAir に設定できます。

次に、アクセス ポイントの Cisco CleanAir を有効にする例を示します。

```
(Cisco Controller) >config 802.11-abgn cleanair enable AP3600 band 5
```

config 802.11a 11acsupport

802.11ac 5 GHz パラメータを設定するには、次のコマンドを使用します： **config 802.11a 11acsupport**

config 802.11a 11acsupport {**enable** | **disable** | **mcs tx** *mcs_index* **ss** *spatial_stream* {**enable** | **disable**}}

構文の説明

enable	802.11ac 5 GHz モードを有効にします。
disable	802.11ac 5 GHz モードを無効にします。
mcs tx	データをアクセス ポイントとクライアント間で送信できる 802.11ac 5 GHz 変調および符号化方式（MCS）レートを設定します。
tx	802.11ac 5 GHz MCS 送信レートを設定します。
mcs_index	MCS インデックス値（8 または 9）。インデックス 8 または 9 の MCS データ レートは、802.11ac 固有です。インデックス 9 の MCS データ レートを有効にすると、自動的に MCS インデックス 8 のデータ レートが有効になります。
ss	802.11ac 5 GHz MCS 空間ストリーム（SS）を設定します。
spatial_stream	MCS データ レートを有効または無効にできる空間ストリーム。 さまざまなアンテナによって送信される信号は、同じスペクトル チャネル内の異なる空間を使用することによって多重化されます。これらの空間は「空間ストリーム」と呼ばれます。MCS レートを有効または無効にできる 3 つの空間ストリームを利用できます。有効な範囲は 1 ～ 3 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

802.11n/ac モードの無効化は、アクセス無線だけに適用されます。バックホール無線は、802.11n に対応している場合、常に 802.11n/ac モードを有効にします。

次に、空間ストリーム 3 の MCS インデックスを設定する例を示します。

```
(Cisco Controller) >config 802.11a 11acsupport mcs tx 9 ss 3
```

config 802.11-a antenna extAntGain

アクセス ポイントに対して 4.9 GHz および 5.8 GHz Public Safety チャネルの外部アンテナ ゲインを設定するには、**config 802.11-a antenna extAntGain** コマンドを使用します。

config {**802.11-a49** | **802.11-a58**} **antenna extAntGain** *ant_gain cisco_ap* {**global** | *channel_no*}

構文の説明

802.11-a49	4.9 GHz Public Safety チャネルを指定します。
802.11-a58	5.8 GHz Public Safety チャネルを指定します。
ant_gain	0.5 dBi 単位の値（例：2.5 dBi = 5）
cisco_ap	このコマンドを適用するアクセス ポイントの名前。
global	すべてのチャネルにアンテナ ゲイン値を指定します。
channel_no	特定のチャネルのアンテナ ゲイン値。

コマンド デフォルト

チャネル プロパティは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config 802.11-a antenna extAntGain コマンドを入力する前に、**config 802.11-a disable** コマンドでシスコの 802.11 対応無線を無効にします。

外部アンテナ ゲインを設定した後に、**config 802.11-a enable** コマンドを使用してシスコの 802.11 対応無線を再び有効にします。

次に、802.11-a49 外部アンテナ ゲインとして 10 dBi を AP1 に設定する例を示します。

```
(Cisco Controller) >config 802.11-a antenna extAntGain 10 AP1
```

config 802.11-a channel ap

アクセス ポイントに対して 4.9 GHz および 5.8 GHz Public Safety チャネルのチャネル特性を設定するには、**config 802.11-a channel ap** コマンドを使用します。

config {**802.11-a49** | **802.11-a58**} **channel ap** *cisco_ap* {**global** | *channel_no*}

構文の説明

802.11-a49	4.9 GHz Public Safety チャネルを指定します。
802.11-a58	5.8 GHz Public Safety チャネルを指定します。
cisco_ap	このコマンドを適用するアクセス ポイントの名前。
global	すべての 4.9 GHz および 5.8 GHz サブ帯域無線に対して動的なチャネル割り当て（DCA）を有効にします。
channel_no	特定のメッシュ アクセス ポイントのカスタム チャネル。範囲は、4.9 GHz 帯域で 1～26、5.8 GHz で 149～165 です。

コマンド デフォルト

チャネル プロパティは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、チャネル プロパティを設定する例を示します。

```
(Cisco Controller) >config 802.11-a channel ap
```

config 802.11-a txpower ap

アクセス ポイントに対して 4.9 GHz および 5.8 GHz Public Safety チャネルの伝送パワー特性を設定するには、**config 802.11-a txpower ap** コマンドを使用します。

config {**802.11-a49** | **802.11-a58**} **txpower ap** *cisco_ap* {**global** | *power_level*}

構文の説明

802.11-a49	4.9 GHz Public Safety チャネルを指定します。
802.11-a58	5.8 GHz Public Safety チャネルを指定します。
txpower	伝送パワー特性を設定します。
ap	アクセス ポイント チャネルを設定します。
cisco_ap	このコマンドを適用するアクセス ポイントの名前。
global	すべてのチャネルに伝送パワー値を適用します。
power_level	指定したメッシュ アクセス ポイントに対する伝送パワー値。指定できる範囲は 1 ～ 5 です。

コマンド デフォルト

アクセス ポイントに対して 4.9 GHz および 5.8 GHz Public Safety チャネルの伝送パワー特性は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11-a49 伝送パワー レベルとして 4 を AP1 に設定する例を示します。

```
(Cisco Controller) >config 802.11-a txpower ap 4 AP1
```

config 802.11 antenna diversity

802.11 アンテナのダイバーシティ オプションを設定するには、**config 802.11 antenna diversity** コマンドを使用します。

config 802.11{**a** | **b**} **antenna diversity** {**enable** | **sideA** | **sideB**} *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	ダイバーシティをイネーブルにします。
sideA	内部アンテナと Cisco Lightweight アクセス ポイントの左ポートに接続されている外部アンテナとの間のダイバーシティを指定します。
sideB	内部アンテナと Cisco Lightweight アクセス ポイントの右ポートに接続されている外部アンテナとの間のダイバーシティを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11b ネットワーク上の AP01 のアンテナ ダイバーシティを有効にする例を示します。

```
(Cisco Controller) >config 802.11a antenna diversity enable AP01
```

次に、Cisco Lightweight アクセス ポイントの左ポート（sideA）に接続されている外部アンテナを使用して、802.11a ネットワーク上の AP01 のダイバーシティを有効にする例を示します。

```
(Cisco Controller) >config 802.11a antenna diversity sideA AP01
```

config 802.11 antenna extAntGain

802.11 ネットワークの外部アンテナ ゲインを設定するには、**config 802.11 antenna extAntGain** コマンドを使用します。

config 802.11{**a** | **b**} **antenna extAntGain** *antenna_gaincisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
antenna_gain	0.5 dBm 単位でアンテナ ゲインを入力します（例：2.5 dBm = 5）。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config 802.11 antenna extAntGain コマンドを入力する前に、**config 802.11 disable** コマンドでシスコの 802.11 対応無線を無効にします。

外部アンテナ ゲインを設定した後に、**config 802.11 enable** コマンドを使用してシスコの 802.11 対応無線を有効にします。

次に、*802.11a* 外部アンテナ ゲインとして *0.5 dBm* を *AP1* に設定する例を示します。

```
(Cisco Controller) >config 802.11 antenna extAntGain 1 AP1
```

config 802.11 antenna mode

802.11 の 180 度セクター化カバレッジ パターンに 1 つの内部アンテナを使用する、または 802.11 の 360 度全方向性カバレッジ パターンに両方の内部アンテナを使用する Cisco Lightweight アクセス ポイントを設定するには、**config 802.11 antenna mode** コマンドを使用します。

config 802.11 {**a** | **b**} **antenna mode** {**omni** | **sectorA** | **sectorB**} *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
omni	両方の内部アンテナを使用するように指定します。
sectorA	サイド A の内部アンテナだけを使用するように指定します。
sectorB	サイド B の内部アンテナだけを使用するように指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、802.11b ネットワーク上でアクセス ポイント AP01 のアンテナを 360 度全方向性パターンに設定する例を示します。

```
(Cisco Controller) >config 802.11 antenna mode omni AP01
```

config 802.11 antenna selection

802.11 ネットワーク上の Cisco Lightweight アクセス ポイントに対して内部アンテナまたは外部アンテナの使用を選択するには、**config 802.11 antenna selection** コマンドを使用します。

config 802.11{**a** | **b**} **antenna selection** {**internal** | **external**} *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
internal	内部アンテナを指定します。
external	外部アンテナを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、内部アンテナを使用する 802.11b ネットワーク上にアクセス ポイント AP02 を設定する例を示します。

```
(Cisco Controller) >config 802.11a antenna selection internal AP02
```

config 802.11b 11gSupport

Cisco Wireless LAN ソリューションの 802.11g ネットワークを有効または無効にするには、**config 802.11b 11gSupport** コマンドを使用します。

config 802.11b 11gSupport {**enable** | **disable**}

構文の説明

enable	802.11g ネットワークを有効にします。
disable	802.11g ネットワークを無効にします。

コマンド デフォルト

Cisco Wireless LAN ソリューションの 802.11g のネットワークは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config 802.11b 11gSupport {**enable** | **disable**} コマンドを入力する前に、**config 802.11 disable** コマンドでシスコの 802.11 対応無線を無効にします。

802.11g ネットワークのサポートを設定後、**config 802.11 enable** コマンドを使用して 802.11 無線を有効にします。

（注） 個々の無線 LAN で 802.11a、802.11b および 802.11g ネットワークを無効にするには、**config wlan radio** コマンドを使用します。

次に、802.11g ネットワークを有効にする例を示します。

```
(Cisco Controller) > config 802.11b 11gSupport enable
Changing the 11gSupport will cause all the APs to reboot when you enable
 802.11b network.
Are you sure you want to continue? (y/n) n
11gSupport not changed!
```

config 802.11b preamble

サブクローズ 18.2.2.2 で定義されている 802.11b プリアンブルを **long**（遅いが信頼性が高い）または **short**（速いが信頼性が低い）に変更するには、**config 802.11b preamble** コマンドを使用します。

config 802.11b preamble {**long** | **short**}

構文の説明

long	long 802.11b プリアンブルを指定します。
short	short 802.11b プリアンブルを指定します。

コマンド デフォルト

802.11b プリアンブルのデフォルト値は short です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

（注） このコマンドを実装するには、保存して Cisco ワイヤレス LAN コントローラをリブート（システムをリセット）する必要があります。

SpectraLink 社の NetLink 電話など、一部のクライアント向けに Cisco ワイヤレス LAN コントローラを最適化するには、このパラメータを **long** に設定する必要があります。

このコマンドは、CLI インターフェイスがアクティブなときはいつでも使用できます。

次に、802.11b プリアンブルを short に変更する例を示します。

```
(Cisco Controller) >config 802.11b preamble short
(Cisco Controller) >(reset system with save)
```

config 802.11h channelswitch

802.11h チャネル スイッチ通知を設定するには、**config 802.11h channelswitch** コマンドを使用します。

config 802.11h channelswitch {**enable** {**loud** | **quiet**} | **disable**}

構文の説明

enable	802.11h チャネル スイッチ通知をイネーブルにします。
loud	802.11h チャネル スイッチ通知を loud モードで有効にします。802.11h が有効になっているクライアントは、チャネルの切り替え中にパケットを送信できます。
quiet	干渉を減らすためにレーダーおよびクライアント デバイスも送信を終了する必要があることを AP が検出した場合に、802.11hが有効になっているクライアントがパケット送信をただちに停止できるようにします。
disable	802.11h チャネル スイッチ通知をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	• このコマンドは、リリース 7.6 以前のリリースで導入されました。 • **loud** パラメータと **quiet** パラメータが導入されました。

次に、802.11h スイッチ通知を無効にする例を示します。

```
(Cisco Controller) >config 802.11h channelswitch disable
```

config 802.11h powerconstraint

802.11h の電力制限値を設定するには、**config 802.11h powerconstraint** コマンドを使用します。

config 802.11h powerconstraint *value*

構文の説明

value	802.11h の電力制限値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11h 電力制限を 5 に設定する例を示します。

```
(Cisco Controller) >config 802.11h powerconstraint 5
```

config 802.11h setchannel

802.11h チャネル通知を使用して新規チャネルを設定するには、**config 802.11h setchannel** コマンドを使用します。

config 802.11h setchannel *cisco_ap*

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11h チャネルを使用して新しいチャネルを設定する例を示します。

```
(Cisco Controller) >config 802.11h setchannel ap02
```

config 802.11 11nsupport

ネットワークで 802.11n のサポートを有効にするには、**config 802.11 11nsupport** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport** {**enable** | **disable**}

構文の説明

a	802.11a ネットワーク設定を指定します。
b	802.11b/g ネットワーク設定を指定します。
enable	802.11n サポートをイネーブルにします。
disable	802.11n サポートをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークで 802.11n のサポートを有効にする例を示します。

```
(Cisco Controller) >config 802.11a 11nsupport enable
```

config 802.11 11nsupport a-mpdu tx priority

802.11n パケットに対して使用される集約方法を指定するには、**config 802.11 11nsupport a-mpdu tx priority** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport a-mpdu tx priority** {**0-7** | **all**} {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
0-7	0 ～ 7 の集約 MAC プロトコル データ ユニットの優先度を指定します。
all	すべての優先度を一度に設定します。
enable	優先度に関連付けられたトラフィックが A-MPDU 伝送を使用するように指定します。
disable	優先度に関連付けられたトラフィックが A-MSDU 伝送を使用するように指定します。

コマンド デフォルト

優先度 0 が有効になっています。

使用上のガイドライン

集約は、パケット データ フレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約方法には、Aggregated MAC Protocol Data Unit（A-MPDU）と Aggregated MAC Service Data Unit（A-MSDU）の 2 種類があります。A-MPDU はソフトウェアで実行されますが、A-MSDU はハードウェアで実行されます。

トラフィック タイプごとに割り当てられた集約 MAC プロトコル データ ユニットの優先度は次のとおりです。

- 1：バックグラウンド
- 2：スペア
- 0：ベスト エフォート
- 3：エクセレント エフォート
- 4：制御ロード
- 5：ビデオ（100 ms 未満の遅延およびジッタ）
- 6：音声（10 ms 未満の遅延およびジッタ）
- 7：ネットワーク コントロール
- all：すべての優先度を一度に設定します。

（注） クライアントが使用する集約方法に合わせて優先度を設定します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、優先度に関連付けられたトラフィックがA-MSDU伝送を使用するようにすべての優先度を設定する例を示します。

```
(Cisco Controller) >config 802.11a 11nsupport a-mpdu tx priority all enable
```

config 802.11 11nsupport a-mpdu tx scheduler

802.11n-5 GHz A-MPDU 伝送集約スケジューラを設定するには、**config 802.11 11nsupport a-mpdu tx scheduler** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport a-mpdu tx scheduler** {**enable** | **disable** | **timeout rt** *timeout-value*}

構文の説明

enable	802.11n-5 GHz A-MPDU 伝送集約スケジューラをイネーブルにします。
disable	802.11n-5 GHz A-MPDU 伝送集約スケジューラをディセーブルにします。
timeout rt	A-MPDU 伝送集約スケジューラのリアルタイム トラフィック タイムアウトを設定します。
timeout-value	タイムアウト値はミリ秒単位です。有効範囲は 1 ～ 1000 ミリ秒です。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドを入力する前に、802.11 ネットワークがディセーブルであることを確認します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、A-MPDU 伝送集約スケジューラのリアルタイム トラフィック タイムアウトを 100 ミリ秒に設定する例を示します。

```
(Cisco Controller) >config 802.11 11nsupport a-mpdu tx scheduler timeout rt 100
```

config 802.11 11nsupport antenna

特定のアンテナを使用するようにアクセス ポイントを設定するには、**config 802.11 11nsupport antenna** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport antenna** *cisco_ap* {**A** | **B** | **C** | **D**} {**enable** | **disable**}

構文の説明

a	802.11a/n ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
cisco_ap	アクセス ポイント。
A/B/C/D	アンテナ ポートを指定します。
enable	設定をイネーブルにします。
disable	設定をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、レガシー直交周波数分割多重化用の 1 つのアンテナに伝送を設定する例を示します。

```
(Cisco Controller) >config 802.11 11nsupport antenna AP1 C enable
```

config 802.11 11nsupport guard-interval

ガード間隔を設定するには、**config 802.11 11nsupport guard-interval** コマンドを使用します。

config 802.11 {**a** | **b**} **11nsupport guard-interval** {**any** | **long**}

構文の説明

any	短期または長期ガード間隔をイネーブルにします。
long	長期ガード間隔のみをイネーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、長期ガード間隔を設定する例を示します。

```
(Cisco Controller) >config 802.11 11nsupport guard-interval long
```

config 802.11 11nsupport mcs tx

アクセス ポイントとクライアントの間でのデータ伝送に使用される Modulation and Coding Scheme（MCS）レートを指定するには、**config 802.11 11nsupport mcs tx** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport mcs tx** {**0-15**} {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
11nsupport	802.11n デバイスのサポートを指定します。
mcs tx	次のように変調および符号化方式のデータ レートを指定します。 • 0（7 Mbps） • 1（14 Mbps） • 2（21 Mbps） • 3（29 Mbps） • 4（43 Mbps） • 5（58 Mbps） • 6（65 Mbps） • 7（72 Mbps） • 8（14 Mbps） • 9（29 Mbps） • 10（43 Mbps） • 11（58 Mbps） • 12（87 Mbps） • 13（116 Mbps） • 14（130 Mbps） • 15（144 Mbps）
enable	この設定をイネーブルにします。
disable	この設定をディセーブルにします。

コマンド デフォルト　なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MCS レートを指定する例を示します。

```
(Cisco Controller) >config 802.11a 11nsupport mcs tx 5 enable
```

config 802.11 11nsupport rifs

データ フレームとその確認応答の間に Reduced Interframe Space（RIFS）を設定するには、**config 802.11 11nsupport rifs** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport rifs** {**enable** | **disable**}

構文の説明

enable	802.11 ネットワークの RIFS をイネーブルにします。
disable	802.11 ネットワークの RIFS をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RIFS を有効にする例を示します。

```
(Cisco Controller) >config 802.11a 11nsupport rifs enable
```

config 802.11 antenna diversity

802.11 アンテナのダイバーシティ オプションを設定するには、**config 802.11 antenna diversity** コマンドを使用します。

config 802.11{**a** | **b**} **antenna diversity** {**enable** | **sideA** | **sideB**} *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	ダイバーシティをイネーブルにします。
sideA	内部アンテナと Cisco Lightweight アクセス ポイントの左ポートに接続されている外部アンテナとの間のダイバーシティを指定します。
sideB	内部アンテナと Cisco Lightweight アクセス ポイントの右ポートに接続されている外部アンテナとの間のダイバーシティを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11b ネットワーク上の AP01 のアンテナ ダイバーシティを有効にする例を示します。

```
(Cisco Controller) >config 802.11a antenna diversity enable AP01
```

次に、Cisco Lightweight アクセス ポイントの左ポート（sideA）に接続されている外部アンテナを使用して、802.11a ネットワーク上の AP01 のダイバーシティを有効にする例を示します。

```
(Cisco Controller) >config 802.11a antenna diversity sideA AP01
```

config 802.11 antenna extAntGain

802.11 ネットワークの外部アンテナ ゲインを設定するには、**config 802.11 antenna extAntGain** コマンドを使用します。

config 802.11{**a** | **b**} **antenna extAntGain** *antenna_gaincisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
antenna_gain	0.5 dBm 単位でアンテナ ゲインを入力します（例：2.5 dBm = 5）。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config 802.11 antenna extAntGain コマンドを入力する前に、**config 802.11 disable** コマンドでシスコの 802.11 対応無線を無効にします。

外部アンテナ ゲインを設定した後に、**config 802.11 enable** コマンドを使用してシスコの 802.11 対応無線を有効にします。

次に、*802.11a* 外部アンテナ ゲインとして *0.5 dBm* を *AP1* に設定する例を示します。

```
(Cisco Controller) >config 802.11 antenna extAntGain 1 AP1
```

config 802.11 antenna mode

802.11 の 180 度セクター化カバレッジ パターンに 1 つの内部アンテナを使用する、または 802.11 の 360 度全方向性カバレッジ パターンに両方の内部アンテナを使用する Cisco Lightweight アクセス ポイントを設定するには、**config 802.11 antenna mode** コマンドを使用します。

config 802.11{**a** | **b**} **antenna mode** {**omni** | **sectorA** | **sectorB**} *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
omni	両方の内部アンテナを使用するように指定します。
sectorA	サイド A の内部アンテナだけを使用するように指定します。
sectorB	サイド B の内部アンテナだけを使用するように指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、802.11b ネットワーク上でアクセス ポイント AP01 のアンテナを 360 度全方向性パターンに設定する例を示します。

```
(Cisco Controller) >config 802.11 antenna mode omni AP01
```

config 802.11 antenna selection

802.11 ネットワーク上の Cisco Lightweight アクセス ポイントに対して内部アンテナまたは外部アンテナの使用を選択するには、**config 802.11 antenna selection** コマンドを使用します。

config 802.11{**a** | **b**} **antenna selection** {**internal** | **external**} *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
internal	内部アンテナを指定します。
external	外部アンテナを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、内部アンテナを使用する 802.11b ネットワーク上にアクセス ポイント AP02 を設定する例を示します。

```
(Cisco Controller) >config 802.11a antenna selection internal AP02
```

config 802.11 channel

802.11 ネットワークまたは単一アクセス ポイントで自動または手動チャネル選択を設定するには、**config 802.11 channel** コマンドを使用します。

config 802.11 {**a** | **b**} **channel** {**global** [**auto** | **once** | **off** | **restart**]} | **ap** {*ap_name* [**global** | *channel*]}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	RRM によって自動的に設定される 802.11a 動作チャネルを指定し、既存の設定を上書きします。
auto	（任意）802.11a 無線のチャネルが無線リソース管理（RRM）によって自動的に設定されるように指定します。
once	（任意）チャネルが RRM によって一度だけ自動的に設定されるように指定します。
off	（任意）RRM による自動チャネル選択が無効化されるように指定します。
restarts	（任意）アグレッシブ DCA サイクルを再開します。
ap_name	アクセス ポイント名。
channel	アクセス ポイントで使用される手動チャネル番号。サポートされるチャネルは、使用されるアクセス ポイントおよび規制区域によって異なります。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

単一 Lightweight アクセス ポイントで 802.11 チャネルを設定する場合、**config 802.11 disable** コマンドを入力して 802.11 ネットワークを無効にします。**config 802.11 channel** コマンドを入力して、無線リソース管理（RRM）による自動チャネル選択を設定するか、手動で 802.11 無線

のチャネルを設定し、**config 802.11 enable** コマンドを入力して 802.11 ネットワークを有効にします。

（注） アクセス ポイントでサポートされているチャネルについては、ドキュメント『Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points』を参照してください。パワーレベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。

次に、アベイラビリティおよび干渉に基づいて自動チャネル設定の 802.11a チャネルが RRM によって自動的に設定されるようにする例を示します。

```
(Cisco Controller) >config 802.11a channel global auto
```

次に、アベイラビリティおよび干渉に基づいて 802.11b チャネルを一度だけ設定する例を示します。

```
(Cisco Controller) >config 802.11b channel global once
```

次に、802.11a 自動チャネル設定をオフにする例を示します。

```
(Cisco Controller) >config 802.11a channel global off
```

次に、自動チャネルの設定でアクセス ポイント AP01 に 802.11b チャネルを設定する例を示します。

```
(Cisco Controller) >config 802.11b AP01 channel global
```

次に、デフォルトのチャネルとしてアクセス ポイント AP01 に 802.11a チャネル 36 を設定する例を示します。

```
(Cisco Controller) >config 802.11a channel AP01 36
```

config 802.11 channel ap

アクセス ポイントの通信無線チャネルを設定するには、**config 802.11 channel ap** コマンドを使用します。

config 802.11 {**a** | **b**} **channel ap** *cisco_ap* {**global** | *channel_no*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
cisco_ap	Cisco アクセス ポイントの名前。
global	指定したアクセス ポイント上で自動 RF を有効にします。
channel_no	デフォルトのチャネル（1～26）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11b ネットワーク上のアクセス ポイント AP01 の自動 RF を有効にする例を示します。

```
(Cisco Controller) >config 802.11b channel ap AP01 global
```

config 802.11 chan_width

特定のアクセス ポイントのチャネル幅を設定するには、**config 802.11 chan_width** コマンドを使用します。

config 802.11{**a** | **b**} **chan_width** *cisco_ap* {**20** | **40** | **80** | **160** | **best**}

構文の説明

a	スロット 1 の 802.11a 無線とスロット 2 の 802.11ac 無線を設定します。
b	802.11b/g 無線を指定します。
cisco_ap	アクセス ポイント。
20	20 MHz チャネルだけを使用する無線の通信を許可します。 20 MHz チャネルだけを使用して通信するレガシー 802.11a 無線、20 MHz 802.11n 無線、または 40 MHz 802.11n 無線の場合にこのオプションを選択します。
40	隣接する 2 つの 20 MHz チャネルを結合して使用する 40 MHz 802.11n 無線の通信を許可します。
80	隣接する 2 つの 40 MHz チャネルを結合して使用する 80 MHz の 802.11ac 無線の通信を許可します。
160	160 MHz の 802.11ac 無線の通信を許可します。
best	このモードでは、デバイスが最適な帯域幅チャネルを選択します。

コマンド デフォルト

デフォルトのチャネル幅は 20 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.3	このコマンドは、160 MHz および最適なチャネル帯域幅のモードを含むように、このリリースで拡張されました。

使用上のガイドライン

このパラメータは、プライマリ チャネルが静的に割り当てられている場合にだけ設定できます。

⚠

注意 2.4 GHz 無線帯域内で 40 MHz チャネルを設定することは、重大な同一チャネル干渉を発生させる可能性があるため推奨されません。

アクセス ポイントの無線を 20 MHz モードまたは 40 MHz モードに静的に設定すると、グローバルに設定されている動的なチャネル割り当て（DCA）チャネル幅の設定（**config advanced 802.11 channel dca chan-width** コマンドを使用して設定）は上書きされます。このアクセス ポイントの無線に対する静的な設定をグローバルに戻すように変更すると、それまでアクセス ポイントで使用されていたチャネル幅がグローバルな DCA 設定で上書きされます。

次に、40 MHz チャネルを使用して 802.11 ネットワークでアクセス ポイント AP01 のチャネル幅を設定する例を示します。

```
(Cisco Controller) >config 802.11a chan_width AP01 40
```

config 802.11 rx-sop threshold

各 802.11 帯域の RxSOP（Receiver Start of Packet Detection Threshold）のしきい値を設定するには、**config 802.11 rx-sop threshold** コマンドを使用します。

config {**802.11a** | **802.11b**} **rx-sop threshold** {**high** | **medium** | **low** | **auto**} {**ap** *ap_name* | **default**}

構文の説明

802.11a	802.11a ネットワークの RxSOP しきい値を設定します。
802.11b	802.11b ネットワークの RxSOP しきい値を設定します。
high	802.11a/b ネットワークの高レベルの RxSOP しきい値を設定します。
medium	802.11a/b ネットワークの中レベルの RxSOP しきい値を設定します。
low	802.11a/b ネットワークの低レベルの RxSOP しきい値を設定します。
auto	802.11a/b ネットワークの自動 RxSOP しきい値を設定します。auto を選択すると、アクセス ポイントが最適な RxSOP しきい値を決定します。
ap *ap_name*	802.11 ネットワークのアクセス ポイントで RxSOP しきい値を設定します。
default	802.11 ネットワークのすべてのアクセス ポイントで RxSOP しきい値を設定します。

コマンド デフォルト

デフォルトの RxSOP しきい値オプションは auto です。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

RxSOP は、アクセス ポイントの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。レベルが高いほど、無線機の感度が低く、レシーバ セル サイズが小さくなります。次の表に、各 802.11 帯域の高、中、低レベルの RxSOP しきい値を示します。

表 *3 : RxSOP* しきい値

802.11 帯	高しきい値	中しきい値	低しきい値
5 GHz	–76 dBm	-78 dBm	–80 dBm
2.4 GHz	–79 dBm	–82 dBm	–85 dBm

次に、802.11a 帯域のすべてのアクセス ポイントに関して高レベルの RxSOP しきい値を設定する例を示します。

```
(Cisco Controller) > config 802.11a rx-sop threshold high
```

config 802.11 txPower

802.11 ネットワーク内のすべてのアクセス ポイントまたは単一アクセス ポイントに対して伝送パワー レベルを設定するには、**config 802.11 txPower** コマンドを使用します。

config 802.11 {**a** | **b**} **txPower** {**global** {*power_level* | **auto** | **max** | **min** | **once** } | **ap** *cisco_ap*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての Lightweight アクセス ポイントに対して 802.11 伝送パワー レベルを設定します。
auto	（任意）シスコの 802.11 対応無線のパワー レベルが無線リソース管理（RRM）によって自動的に設定されるように指定します。
once	（任意）パワー レベルが RRM によって一度だけ自動的に設定されるように指定します。
power_level	（任意）アクセス ポイントに手動で設定する伝送パワー レベルの数値。
ap	指定した Lightweight アクセス ポイントに対して 802.11 伝送パワー レベルを設定します。
ap_name	アクセス ポイント名。

コマンド デフォルト

コマンドのデフォルト（**global**、**auto**）は RRM による自動設定用です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての Lightweight アクセス ポイントで 802.11a 無線の伝送パワー レベルを自動的に設定する例を示します。

```
(Cisco Controller) > config 802.11a txPower auto
```

次に、すべての Lightweight アクセス ポイントに 802.11b 無線の伝送パワーを手動でレベル 5 に設定する例を示します。

```
(Cisco Controller) > config 802.11b txPower global 5
```

次に、アクセス ポイント AP1 で 802.11b 無線の伝送パワーを自動的に設定する例を示します。

```
(Cisco Controller) > config 802.11b txPower AP1 global
```

次に、アクセス ポイント AP1 に 802.11a 無線の伝送パワーを手動でレベル 2 に設定する例を示します。

```
(Cisco Controller) > config 802.11b txPower AP1 2
```

関連コマンド

show ap config 802.11a

config 802.11b txPower

config 802.11 beamforming

ネットワークまたは個々の無線に対してビームフォーミング（ClientLink）を有効または無効にするには、**config 802.11 beamforming** コマンドを入力します。

config 802.11{**a** | **b**} **beamforming** {**global** | **ap** *ap_name* } {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての Lightweight アクセス ポイントを指定します。
ap *ap_name*	Cisco アクセス ポイント名を指定します。
enable	ビームフォーミングを有効にします。
disable	ビームフォーミングを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ネットワークに対してビームフォーミングを有効にすると、そのネットワーク タイプに対応するすべての無線に対してビームフォーミングが自動的に有効になります。

ビームフォーミングを使用する際は、次のガイドラインに従ってください。

- ビームフォーミングは、レガシー直交周波数分割多重（OFDM）データ レート（6、9、12、18、24、36、48、および 54 mbps）でだけサポートされています。

（注） ビームフォーミングは、相補型符号変調（CCK）データ レート（1、2、5.5、および 11 Mbps）ではサポートされていません。

- ビームフォーミングは、802.11n に対応したアクセス ポイント（AP1250 および AP1140）でだけサポートされます。
- 送信用に 2 本以上のアンテナを有効にする必要があります。
- 受信用に 3 本すべてのアンテナを有効にする必要があります。
- OFDM レートを有効にする必要があります。

送信アンテナがアンテナ設定により 1 本に制限されている場合、あるいは OFDM レートが無効になっている場合、ビームフォーミングは使用されません。

次に、802.11a ネットワーク上でビームフォーミングを有効にする例を示します。

```
(Cisco Controller) >config 802.11 beamforming global enable
```

config 802.11h channelswitch

802.11h チャネル スイッチ通知を設定するには、**config 802.11h channelswitch** コマンドを使用します。

config 802.11h channelswitch {**enable** {**loud** | **quiet**} | **disable**}

構文の説明

enable	802.11hチャネル スイッチ通知をイネーブルにします。
loud	802.11h チャネル スイッチ通知を loud モードで有効にします。802.11h が有効になっているクライアントは、チャネルの切り替え中にパケットを送信できます。
quiet	干渉を減らすためにレーダーおよびクライアント デバイスも送信を終了する必要があることを AP が検出した場合に、802.11hが有効になっているクライアントがパケット送信をただちに停止できるようにします。
disable	802.11hチャネル スイッチ通知をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	• このコマンドは、リリース 7.6 以前のリリースで導入されました。 • **loud** パラメータと **quiet** パラメータが導入されました。

次に、802.11h スイッチ通知を無効にする例を示します。

```
(Cisco Controller) >config 802.11h channelswitch disable
```

config 802.11h powerconstraint

802.11h の電力制限値を設定するには、**config 802.11h powerconstraint** コマンドを使用します。

config 802.11h powerconstraint *value*

構文の説明

value	802.11h の電力制限値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11h 電力制限を 5 に設定する例を示します。

```
(Cisco Controller) >config 802.11h powerconstraint 5
```

config 802.11h setchannel

802.11h チャネル通知を使用して新規チャネルを設定するには、**config 802.11h setchannel** コマンドを使用します。

config 802.11h setchannel *cisco_ap*

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11h チャネルを使用して新しいチャネルを設定する例を示します。

```
(Cisco Controller) >config 802.11h setchannel ap02
```

config 802.11h smart dfs

802.11h smart-dfs 機能を有効または無効にするには、**config 802.11h smart-dfs** コマンドを使用します。

config 802.11h smart-dfs {**enable** | **disable**}

構文の説明

enable	レーダー干渉チャネルの非占有時間の倍増を有効にします。
disable	非占有時間の倍増を無効にして、レーダー干渉チャネルの従来の時間（30 分）を使用します。 従来の DFS の動作に適合させるには disable を使用してください。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
8.2.141.0	このコマンドが導入されました。

次に、802.11h smart-dfs を有効にする例を示します。

```
(Cisco Controller) >config 802.11h smart-dfs enable
```

config 802.11 11nsupport

ネットワークで 802.11n のサポートを有効にするには、**config 802.11 11nsupport** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport** {**enable** | **disable**}

構文の説明

a	802.11a ネットワーク設定を指定します。
b	802.11b/g ネットワーク設定を指定します。
enable	802.11n サポートをイネーブルにします。
disable	802.11n サポートをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークで 802.11n のサポートを有効にする例を示します。

```
(Cisco Controller) >config 802.11a 11nsupport enable
```

config 802.11 11nsupport a-mpdu tx priority

802.11n パケットに対して使用される集約方法を指定するには、**config 802.11 11nsupport a-mpdu tx priority** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport a-mpdu tx priority** {**0-7** | **all**} {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
0-7	0 ～ 7 の集約 MAC プロトコル データ ユニットの優先度を指定します。
all	すべての優先度を一度に設定します。
enable	優先度に関連付けられたトラフィックが A-MPDU 伝送を使用するように指定します。
disable	優先度に関連付けられたトラフィックが A-MSDU 伝送を使用するように指定します。

コマンド デフォルト

優先度 0 が有効になっています。

使用上のガイドライン

集約は、パケット データ フレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約方法には、Aggregated MAC Protocol Data Unit（A-MPDU）と Aggregated MAC Service Data Unit（A-MSDU）の 2 種類があります。A-MPDU はソフトウェアで実行されますが、A-MSDU はハードウェアで実行されます。

トラフィック タイプごとに割り当てられた集約 MAC プロトコル データ ユニットの優先度は次のとおりです。

- 1：バックグラウンド
- 2：スペア
- 0：ベスト エフォート
- 3：エクセレント エフォート
- 4：制御ロード
- 5：ビデオ（100 ms 未満の遅延およびジッタ）
- 6：音声（10 ms 未満の遅延およびジッタ）
- 7：ネットワーク コントロール
- all：すべての優先度を一度に設定します。

（注） クライアントが使用する集約方法に合わせて優先度を設定します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、優先度に関連付けられたトラフィックがA-MSDU伝送を使用するようにすべての優先度を設定する例を示します。

```
(Cisco Controller) >config 802.11a 11nsupport a-mpdu tx priority all enable
```

config 802.11 11nsupport a-mpdu tx scheduler

802.11n-5 GHz A-MPDU 伝送集約スケジューラを設定するには、**config 802.11 11nsupport a-mpdu tx scheduler** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport a-mpdu tx scheduler** {**enable** | **disable** | **timeout rt** *timeout-value*}

構文の説明

enable	802.11n-5 GHz A-MPDU 伝送集約スケジューラをイネーブルにします。
disable	802.11n-5 GHz A-MPDU 伝送集約スケジューラをディセーブルにします。
timeout rt	A-MPDU 伝送集約スケジューラのリアルタイム トラフィック タイムアウトを設定します。
timeout-value	タイムアウト値はミリ秒単位です。有効範囲は 1 ～ 1000 ミリ秒です。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドを入力する前に、802.11 ネットワークがディセーブルであることを確認します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、A-MPDU 伝送集約スケジューラのリアルタイム トラフィック タイムアウトを 100 ミリ秒に設定する例を示します。

```
(Cisco Controller) >config 802.11 11nsupport a-mpdu tx scheduler timeout rt 100
```

config 802.11 11nsupport antenna

特定のアンテナを使用するようにアクセス ポイントを設定するには、**config 802.11 11nsupport antenna** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport antenna** *cisco_ap* {**A** | **B** | **C** | **D**} {**enable** | **disable**}

構文の説明

a	802.11a/n ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
cisco_ap	アクセス ポイント。
A/B/C/D	アンテナ ポートを指定します。
enable	設定をイネーブルにします。
disable	設定をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、レガシー直交周波数分割多重化用の 1 つのアンテナに伝送を設定する例を示します。

```
(Cisco Controller) >config 802.11 11nsupport antenna AP1 C enable
```

config 802.11 11nsupport guard-interval

ガード間隔を設定するには、**config 802.11 11nsupport guard-interval** コマンドを使用します。

config 802.11 {**a** | **b**} **11nsupport guard-interval** {**any** | **long**}

構文の説明

any	短期または長期ガード間隔をイネーブルにします。
long	長期ガード間隔のみをイネーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、長期ガード間隔を設定する例を示します。

```
(Cisco Controller) >config 802.11 11nsupport guard-interval long
```

config 802.11 11nsupport mcs tx

アクセス ポイントとクライアントの間でのデータ伝送に使用される Modulation and Coding Scheme（MCS）レートを指定するには、**config 802.11 11nsupport mcs tx** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport mcs tx** {**0-15**} {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
11nsupport	802.11n デバイスのサポートを指定します。
mcs tx	次のように変調および符号化方式のデータ レートを指定します。 • 0（7 Mbps） • 1（14 Mbps） • 2（21 Mbps） • 3（29 Mbps） • 4（43 Mbps） • 5（58 Mbps） • 6（65 Mbps） • 7（72 Mbps） • 8（14 Mbps） • 9（29 Mbps） • 10（43 Mbps） • 11（58 Mbps） • 12（87 Mbps） • 13（116 Mbps） • 14（130 Mbps） • 15（144 Mbps）
enable	この設定をイネーブルにします。
disable	この設定をディセーブルにします。

コマンド デフォルト　なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MCS レートを指定する例を示します。

```
(Cisco Controller) >config 802.11a 11nsupport mcs tx 5 enable
```

config 802.11 11nsupport rifs

データ フレームとその確認応答の間に Reduced Interframe Space（RIFS）を設定するには、**config 802.11 11nsupport rifs** コマンドを使用します。

config 802.11{**a** | **b**} **11nsupport rifs** {**enable** | **disable**}

構文の説明

enable	802.11 ネットワークの RIFS をイネーブルにします。
disable	802.11 ネットワークの RIFS をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RIFS を有効にする例を示します。

```
(Cisco Controller) >config 802.11a 11nsupport rifs enable
```

config 802.11 beacon period

802.11a、802.11b、または他のサポートされる 802.11 ネットワークに対してビーコン周期をグローバルに変更するには、**config 802.11 beacon period** コマンドを使用します。

config 802.11 {**a** | **b**} **beacon period** *time_units*

（注） このコマンドを使用する前に、802.11 ネットワークを無効にします。「使用上のガイドライン」の項を参照してください。

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
time_units	時間単位（TU）でのビーコン間隔。1 TU は 1024 マイクロ秒です。

コマンド デフォルト

なし

使用上のガイドライン

Cisco Wireless LAN ソリューションの 802.11 ネットワークでは、すべての Cisco Lightweight アクセス ポイント（無線 LAN）が定期的にビーコンをブロードキャストします。このビーコンは、クライアントに 802.11a サービスが使用可能なことを通知し、クライアントは Lightweight アクセス ポイントと同期できます。

ビーコン期間を変更する前に、**config 802.11 disable** コマンドを使用して 802.11 ネットワークを無効にしてください。ビーコン期間を変更した後、**config 802.11 enable** コマンドを使用して 802.11 ネットワークを有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、120 時間単位のビーコン周期に合わせて 802.11a ネットワークを設定する例を示します。

```
(Cisco Controller) > config 802.11 beacon period 120
```

関連コマンド

show 802.11a

config 802.11b beaconperiod

config 802.11a disable

config 802.11a enable

config 802.11 cac defaults

802.11a および 802.11b/g ネットワークのデフォルトの Call Admission Control（CAC）パラメータを設定するには、**config 802.11 cac defaults** コマンドを使用します。

config 802.11 {**a** | **b**} **cac defaults**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

使用上のガイドライン

802.11a または 802.11b/g ネットワークでのビデオ アプリケーションに対して CAC コマンドを実行するには、変更しようとしている WLAN に Wi-Fi Multimedia（WMM）プロトコルが設定され、また Quality of Service（QoS）のレベルが Gold にセットされている必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークのデフォルト CAC パラメータを設定する例を示します。

```
(Cisco Controller) > config 802.11 cac defaults
```

関連コマンド

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac media-stream

config 802.11 cac multimedia

config 802.11 cac video cac-method

debug cac

config 802.11 cac video acm

802.11a または 802.11b/g ネットワークに対してビデオ コール アドミッション制御（CAC）を有効または無効にするには、**config 802.11 cac video acm** コマンドを使用します。

config 802.11{**a** | **b**} **cac video acm** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	ビデオ CAC 設定をイネーブルにします。
disable	ビデオ CAC 設定をディセーブルにします。

コマンド デフォルト

802.11a ネットワークまたは 802.11b/g ネットワークのビデオ CAC 設定はデフォルトでは無効になっています。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11**{**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- **save config** コマンドを入力して、新しい設定を保存します。
- **config 802.11**{**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11**{**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークのビデオ CAC を有効にする例を示します。

```
(Cisco Controller) > config 802.11 cac video acm enable
```

次に、802.11b ネットワークのビデオ CAC を無効にする例を示します。

```
(Cisco Controller) > config 802.11 cac video acm disable
```

関連コマンド

config 802.11 cac video max-bandwidth

config 802.11 cac video roam-bandwidth

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video cac-method

802.11a または 802.11b/g ネットワークでのビデオ アプリケーションの Call Admission Control（CAC）方式を設定するには、**config 802.11 cac video cac-method** コマンドを使用します。

config 802.11 {**a** | **b**} **cac video cac-method** {**static** | **load-based**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
static	802.11a または 802.11b/g ネットワークでのビデオ アプリケーションのスタティック CAC 方式をイネーブルにします。 スタティックまたは帯域幅ベースの CAC を使用して、クライアントは、新しいビデオ要求を受け入れるためにどの程度の帯域幅と共有メディア時間が必要であるかを指定することができ、その結果、要求に対処できるかどうかを判別するためのアクセス ポイントを使用できるようになります。
load-based	802.11a または 802.11b/g ネットワークでのビデオ アプリケーションの負荷ベースの CAC 方式をイネーブルにします。 負荷ベースの CAC またはダイナミック CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。負荷ベースの CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。アクセス ポイントは、コールをサポートするのに十分なだけの未使用帯域幅がチャネルにある場合に限り、新規のコールを許可します。 SIP-CAC がイネーブルのときは、負荷ベースの CAC はサポートされません。

コマンド デフォルト

Static

使用上のガイドライン

802.11a または 802.11b/g ネットワークでのビデオ アプリケーションに対して CAC コマンドを実行するには、変更しようとしている WLAN に Wi-Fi Multimedia（WMM）プロトコルが設定され、また Quality of Service（QoS）のレベルが Gold にセットされている必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。

- **config 802.11{a | b} disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- **save config** コマンドを入力して、新しい設定を保存します。
- **config 802.11{a | b} cac voice acm enable** コマンドまたは **config 802.11{a | b} cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

ビデオ CAC は、ユニキャスト ビデオ CAC と MC2UC CAC の 2 つのパートで構成されています。ユニキャスト ビデオ CAC だけが必要な場合は、スタティック モードだけを設定します。MC2UC CAC だけが必要な場合は、スタティックまたは負荷ベースの CAC を設定します。SIP-CAC がイネーブルのときは、負荷ベースの CAC はサポートされません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークでビデオ アプリケーションのスタティック CAC 方式をイネーブルにする例を示します。

```
(Cisco Controller) > config 802.11 cac video cac-method static
```

関連コマンド

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac defaults

config 802.11 cac media-stream

config 802.11 cac multimedia

debug cac

config 802.11 cac video load-based

802.11a または 802.11b/g ネットワーク上でビデオ アプリケーションに対して負荷ベースの Admission Control（CAC）を有効または無効にするには、**config 802.11 cac video load-based** コマンドを使用します。

config 802.11 {**a** | **b**} **cac video load-based** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	802.11a または 802.11b/g ネットワーク上でビデオ アプリケーションの負荷ベースの CAC をイネーブルにします。 負荷ベースの CAC またはダイナミック CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。負荷ベースの CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。アクセス ポイントは、コールをサポートするのに十分なだけの未使用帯域幅がチャネルにある場合に限り、新規のコールを許可します。
disable	802.11a または 802.11b/g ネットワークのビデオ アプリケーションの負荷ベースの CAC 方式をディセーブルにします。

コマンド デフォルト

ディセーブル

使用上のガイドライン

802.11a または 802.11b/g ネットワークでのビデオ アプリケーションに対して CAC コマンドを実行するには、変更しようとしている WLAN に Wi-Fi Multimedia（WMM）プロトコルが設定され、また Quality of Service（QoS）のレベルが Gold にセットされている必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

ビデオ CAC は、ユニキャスト ビデオ CAC と MC2UC CAC の 2 つのパートで構成されています。ユニキャスト ビデオ CAC だけが必要な場合は、スタティック モードだけを設定します。MC2UC CAC だけが必要な場合は、スタティックまたは負荷ベースの CAC を設定します。SIP-CAC がイネーブルのときは、負荷ベースの CAC はサポートされません。

（注） SIP-CAC がイネーブルのときは、負荷ベースの CAC はサポートされません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークでビデオ アプリケーションに対して負荷ベースの CAC の方式をイネーブルにする例を示します。

```
(Cisco Controller) > config 802.11 cac video load-based enable
```

関連コマンド

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac defaults

config 802.11 cac media-stream

config 802.11 cac multimedia

config 802.11 cac video cac-method

debug cac

config 802.11 cac video max-bandwidth

802.11a または 802.11b/g ネットワーク上でクライアントに割り当てられる最大帯域幅のうち、ビデオ アプリケーション用に使用する割合を設定するには、**config 802.11 cac video max-bandwidth** コマンドを使用します。

config 802.11 {**a** | **b**} **cac video max-bandwidth** *bandwidth*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
bandwidth	5 ～ 85 % の帯域の割合値。

コマンド デフォルト

802.11a または 802.11b/g ネットワークでビデオ アプリケーション用にクライアントに割り当てられるデフォルトの最大帯域幅は、0 % です。

使用上のガイドライン

音声とビデオの最大無線周波数（RF）帯域幅が合計で 85 % を超えてはなりません。クライアントが指定値に達すると、このネットワーク上での新しいコールはアクセス ポイントで拒否されます。

（注） このパラメータがゼロ（0）に設定されている場合、コントローラは帯域幅を割り当てないものと想定して、すべての帯域幅の要求を許可します。

コール アドミッション制御（CAC）コマンドでは、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、選択した無線帯域でビデオ アプリケーションに割り当てられる最大帯域幅の割合を指定する例を示します。

```
(Cisco Controller) > config 802.11 cac video max-bandwidth 50
```

関連コマンド

config 802.11 cac video acm

config 802.11 cac video roam-bandwidth

config 802.11 cac voice stream-size

config 802.11 cac voice roam-bandwidth

config 802.11 cac media-stream

802.11a、802.11b ネットワークのメディア ストリーム Call Admission Control（CAC）の音声とビデオのパラメータを設定するには、**config 802.11 cac media-stream** コマンドを使用します。

config 802.11 {**a** | **b**} **cac media-stream multicast-direct** {**max-retry-percent** *retry-percentage* | **min-client-rate** *dot11-rate*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
multicast-direct	マルチキャスト直接メディア ストリーム用の CAC パラメータを設定します。
max-retry-percent	マルチキャスト直接メディア ストリームに許可される最大再試行回数の割合を設定します。
retry-percentage	マルチキャスト直接メディア ストリームに許可される最大再試行回数の割合。
min-client-rate	マルチキャスト直接メディア ストリーム用のクライアントに最小のデータ送信レートを設定します。
dot11-rate	マルチキャスト直接メディア ストリーム用のクライアントへの最小のデータ送信レート。クライアントが実行できる kbps 単位のレート。 伝送データ レートがこのレートを下回ると、ビデオが起動しないか、クライアントが不良クライアントとして分類される可能性があります。不良クライアント ビデオは、より良いエフォートの QoS のために降格されたり、拒否される可能性があります。使用可能なデータ レートは、6000、9000、12000、18000、24000、36000、48000、54000、および 11n レートです。

コマンド デフォルト

最大再試行回数の割合のデフォルト値は 80 です。80 を超えると、ビデオが開始されないか、クライアントが不良クライアントとして分類される場合があります。不良クライアント ビデオは、より良いエフォートの QoS のために降格されたり、拒否されたりします。

使用上のガイドライン

802.11a または 802.11b/g ネットワークでのビデオ アプリケーションに対して CAC コマンドを実行するには、変更しようとしている WLAN に Wi-Fi Multimedia（WMM）プロトコルが設定され、また Quality of Service（QoS）のレベルが Gold にセットされている必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- **save config** コマンドを入力して、新しい設定を保存します。
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークの 90 としてマルチキャスト直接メディア ストリームの最大試行回数の割合を設定する例を示します。

```
(Cisco Controller) > config 802.11 cac media-stream multicast-direct max-retry-percent
90
```

関連コマンド

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac defaults

config 802.11 cac multimedia

debug cac

config 802.11 cac multimedia

802.11a および 802.11b ネットワークの CAC メディア音声およびビデオ品質パラメータを設定するには、**config 802.11 cac multimedia** コマンドを使用します。

config 802.11 {**a** | **b**} **cac multimedia max-bandwidth** *bandwidth*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
max-bandwidth	802.11a または 802.11b/g ネットワークで音声およびビデオ アプリケーション用に Wi-Fi Multimedia（WMM）クライアントに割り当てられる最大帯域幅の割合を設定します。
bandwidth	802.11a または 802.11b/g ネットワークで音声およびビデオ アプリケーション用に WMM クライアントに割り当てられる最大帯域幅の割合。クライアントが指定値に達すると、アクセス ポイントはこの無線帯域での新しいコールを拒否します。範囲は 5 ～ 85% です。

コマンド デフォルト

802.11a または 802.11b/g ネットワークで音声およびビデオアプリケーション用に Wi-Fi Multimedia（WMM）クライアントに割り当てられるデフォルトの最大帯域幅は、85 % です。

使用上のガイドライン

802.11a または 802.11b/g ネットワークでのビデオ アプリケーションに対して Call Admission Control（CAC）コマンドを実行するには、変更しようとしている WLAN に Wi-Fi Multimedia（WMM）プロトコルが設定され、また Quality of Service（QoS）のレベルが Gold にセットされている必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- **save config** コマンドを入力して、新しい設定を保存します。
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークで音声およびビデオ アプリケーション用に WMM クライアントに割り当てられる最大帯域幅の割合を設定する例を示します。

```
(Cisco Controller) > config 802.11 cac multimedia max-bandwidth 80
```

関連コマンド

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video sip

config 802.11 cac video roam-bandwidth

config 802.11 cac load-based

config 802.11 cac defaults

debug cac

config 802.11 cac video roam-bandwidth

802.11a または 802.11b/g ネットワーク上での最大割り当て帯域幅のうち、ビデオ クライアントのローミング用に予約する割合を設定するには、**config 802.11 cac video roam-bandwidth** コマンドを使用します。

config 802.11 {**a** | **b**} **cac video roam-bandwidth** *bandwidth*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
bandwidth	5 ～ 85 % の帯域の割合値。

コマンド デフォルト

802.11a または 802.11b/g ネットワーク上での最大割り当て帯域幅のうちビデオ クライアントのローミング用に予約されるデフォルトの割合は、0 % です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラは、指定された帯域幅をビデオクライアントのローミング用に最大割り当て帯域幅から予約します。

（注） このパラメータがゼロ（0）に設定されている場合、コントローラは、帯域割り当てが行われないものと想定して、すべての帯域幅の要求を許可します。

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

詳細な手順については、使用しているリリースの『*Cisco Wireless LAN Controller Configuration Guide*』の「Configuring Controller Settings」の章の「Configuring Voice and Video Parameters」の項を参照してください。

次に、選択した無線帯域でビデオ クライアントのローミングに予約された最大割り当て帯域幅の割合を指定する例を示します。

```
(Cisco Controller) > config 802.11 cac video roam-bandwidth 10
```

関連コマンド

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video cac-method

config 802.11 cac video sip

config 802.11 cac video load-based

config 802.11 cac video sip

802.11a または 802.11b/g ネットワーク上でビデオ アプリケーションを使用する非トラフィック仕様（TSPEC）SIP クライアント用のビデオ コール アドミッション制御（CAC）を有効または無効にするには、**config 802.11 cac video sip** コマンドを使用します。

config 802.11 {**a** | **b**} **cac video sip** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	802.11a または 802.11b/g ネットワークでビデオ アプリケーションを使用している非 TSPEC SIP クライアント用のビデオ CAC をイネーブルにします。 非 TSPEC SIP クライアントのビデオ CAC をイネーブルにすると、Facetime コールおよびビデオ コールなどのアプリケーションを使用できます。
disable	802.11a または 802.11b/g ネットワークでビデオ アプリケーションを使用している非 TSPEC SIP クライアント用のビデオ CAC をディセーブルにします。

コマンド デフォルト

なし

使用上のガイドライン

802.11a または 802.11b/g ネットワークでのビデオ アプリケーションに対して CAC コマンドを実行するには、変更しようとしている WLAN に Wi-Fi Multimedia（WMM）プロトコルが設定され、また Quality of Service（QoS）のレベルが Gold にセットされている必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。
- **config wlan call-snoop enable** *wlan_id* コマンドを入力して、SIP クライアントが配置されている WLAN でのコール スヌーピングを有効にします。

次に、802.11a ネットワークでビデオ アプリケーションを使用している非 TSPEC SIP クライアント用のビデオ CAC を有効にする例を示します。

```
(Cisco Controller) > config 802.11 cac video sip enable
```

関連コマンド

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac video cac-method

config 802.11 cac video load-based

config 802.11 cac video roam-bandwidth

config 802.11 cac video tspec-inactivity-timeout

アクセス ポイントから受信したコール アドミッション制御（CAC）の Wi-Fi マルチメディア（WMM）トラフィック仕様（TSPEC）の非アクティブ タイムアウトを処理または無視するには、**config 802.11 cac video tspec-inactivity-timeout** コマンドを使用します。

config 802.11{**a** | **b**} **cac video tspec-inactivity-timeout** {**enable** | **ignore**}

構文の説明

a	802.11a ネットワークを指定します。
ab	802.11b/g ネットワークを指定します。
enable	TSPEC 無活動タイムアウト メッセージを処理します。
ignore	TSPEC 無活動タイムアウト メッセージを無視します。

コマンド デフォルト

アクセス ポイントから受信した CAC の WMM TSPEC の非アクティブ タイムアウトはデフォルトでは無効（無視される）になっています。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11**{**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11**{**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11**{**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、アクセス ポイントから受信した TSPEC 非アクティブ タイムアウト メッセージへの応答を処理する方法を示します。

```
(Cisco Controller) > config 802.11a cac video tspec-inactivity-timeout enable
```

次に、アクセス ポイントから受信した TSPEC 非アクティブ タイムアウト メッセージへの応答を無視する方法を示します。

```
(Cisco Controller) > config 802.11a cac video tspec-inactivity-timeout ignore
```

関連コマンド

config 802.11 cac video acm

config 802.11 cac video max-bandwidth

config 802.11 cac video roam-bandwidth

config 802.11 cac voice acm

802.11a または 802.11b/g ネットワークに対して帯域幅ベースの音声コール アドミッション制御（CAC）を有効または無効にするには、**config 802.11 cac voice acm** コマンドを使用します。

config 802.11 {**a** | **b**} **cac voice acm** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	帯域幅ベースの CAC をイネーブルにします。
disable	帯域幅ベースの CAC をディセーブルにします。

コマンド デフォルト

802.11a または 802.11b/g ネットワーク ID の帯域幅ベースの音声 CAC はデフォルトでは無効になっています。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、帯域幅ベースの CAC をイネーブルにする例を示します。

```
(Cisco Controller) > config 802.11c cac voice acm enable
```

次に、帯域幅ベースの CAC をディセーブルにする例を示します。

```
(Cisco Controller) > config 802.11b cac voice acm disable
```

関連コマンド **config 802.11 cac video acm**

config 802.11 cac voice max-bandwidth

802.11a または 802.11b/g ネットワーク上でクライアントに割り当てられる最大帯域幅のうち、音声アプリケーション用に使用する割合を設定するには、**config 802.11 cac voice max-bandwidth** コマンドを使用します。

config 802.11 {**a** | **b**} **cac voice max-bandwidth** *bandwidth*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
bandwidth	5 ～ 85 % の帯域の割合値。

コマンド デフォルト

802.11a または 802.11b/g ネットワークで音声アプリケーション用にクライアントに割り当てられるデフォルトの最大帯域幅は、0 % です。

使用上のガイドライン

音声とビデオの最大無線周波数（RF）帯域幅が合計で 85 % を超えてはなりません。クライアントが指定値に達すると、このネットワーク上での新しいコールはアクセス ポイントで拒否されます。

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、選択した無線帯域で音声アプリケーションに割り当てられる最大帯域幅の割合を指定する例を示します。

```
(Cisco Controller) > config 802.11a cac voice max-bandwidth 50
```

関連コマンド

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice stream-size

config 802.11 exp-bwreq

config 802.11 tsm

config wlan save

show wlan

show wlan summary

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 cac voice load-based

config 802.11 cac video acm

config 802.11 cac voice roam-bandwidth

802.11a または 802.11b/g ネットワーク上でのコール アドミッション制御（CAC）の最大割り当て帯域幅のうち、音声クライアントのローミング用に予約する割合を設定するには、**config 802.11 cac voice roam-bandwidth** コマンドを使用します。

config 802.11 {**a** | **b**} **cac voice roam-bandwidth** *bandwidth*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
bandwidth	0 ～ 85 % の帯域の割合値。

コマンド デフォルト

802.11a または 802.11b/g ネットワーク上での CAC の最大割り当て帯域幅のうち音声クライアントのローミング用に予約されるデフォルトの割合は、85 % です。

使用上のガイドライン

音声とビデオの最大無線周波数（RF）帯域幅が合計で 85 % を超えてはなりません。コントローラは、指定された帯域幅を音声クライアントのローミング用に最大割り当て帯域幅から予約します。

（注） このパラメータがゼロ（0）に設定されている場合、コントローラは帯域幅を割り当てないものと想定して、すべての帯域幅の要求を許可します。

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、選択した無線帯域で音声クライアントのローミング用に予約された最大割り当て帯域幅の割合を指定する例を示します。

```
(Cisco Controller) > config 802.11 cac voice roam-bandwidth 10
```

関連コマンド

config 802.11 cac voice acm

config 802.11cac voice max-bandwidth

config 802.11 cac voice stream-size

config 802.11 cac voice tspec-inactivity-timeout

アクセス ポイントから受信した Wi-Fi マルチメディア（WMM）トラフィック仕様（TSPEC）の非アクティブ タイムアウトを処理または無視するには、**config 802.11 cac voice tspec-inactivity-timeout** コマンドを使用します。

config 802.11{**a** | **b**} **cac voice tspec-inactivity-timeout** {**enable** | **ignore**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	TSPEC 無活動タイムアウト メッセージを処理します。
ignore	TSPEC 無活動タイムアウト メッセージを無視します。

コマンド デフォルト

アクセス ポイントから受信した WMM TSPEC の非アクティブ タイムアウトはデフォルトでは無効（無視される）になっています。

使用上のガイドライン

コール アドミッション制御（CAC）コマンドでは、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11**{**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- **save config** コマンドを入力して、新しい設定を保存します。
- **config 802.11**{**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11**{**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントから受信した音声 TSPEC 非アクティブ タイムアウト メッセージを有効にする方法を示します。

```
(Cisco Controller) > config 802.11 cac voice tspec-inactivity-timeout enable
```

関連コマンド

config 802.11 cac voice load-based

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice acm

config 802.11cac voice max-bandwidth

config 802.11 cac voice stream-size

config 802.11 cac voice load-based

802.11aまたは802.11b/gネットワークに対して負荷ベースのコールアドミッション制御（CAC）を有効または無効にするには、**config 802.11 cac voice load-based** コマンドを使用します。

config 802.11{**a** | **b**} **cac voice load-based** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	負荷ベースの CAC をイネーブルにします。
disable	負荷ベースのCACをディセーブルにします。

コマンド デフォルト

802.11a ネットワークまたは 802.11b/g ネットワークの負荷ベースの CAC はデフォルトでは無効になっています。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11**{**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11**{**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11**{**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、音声負荷ベースの CAC パラメータを有効にする例を示します。

```
(Cisco Controller) > config 802.11a cac voice load-based enable
```

次に、音声負荷ベースの CAC パラメータを無効にする例を示します。

```
(Cisco Controller) > config 802.11a cac voice load-based disable
```

関連コマンド

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 cac video max-bandwidth

config 802.11 cac video acm

config 802.11 cac voice stream-size

config 802.11 cac voice max-calls

（注） SIP コール スヌーピング機能が無効であるか、SIP ベースのコール アドミッション制御（CAC）の要件が満たされない場合は、**config 802.11 cac voice max-calls** コマンドを使用しないでください。

無線でサポートされる音声コールの最大数を設定するには、**config 802.11 cac voice max-calls** コマンドを使用します。

config 802.11 {**a** | **b**} **cac voice max-calls** *number*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
number	無線ごとに許可するコールの数。

コマンド デフォルト

無線でサポートされる音声コールのデフォルトの最大数は 0 です。これは、コール数の最大制限チェックがないことを意味します。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable network** コマンドを入力して、設定する無線ネットワークを無効にします。
- 次のコマンドを入力して、新しい設定を保存します。 **save config command.**
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、無線でサポートされる音声コールの最大数を設定する例を示します。

```
(Cisco Controller) > config 802.11 cac voice max-calls 10
```

関連コマンド

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice stream-size

config 802.11 exp-bwreq

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 cac voice load-based

config 802.11 cac video acm

config 802.11 cac voice sip bandwidth

（注） SIP 帯域幅とサンプリング間隔は、SIP ベースのコール アドミッション制御（CAC）で、コール帯域幅あたりの計算に使用されます。

802.11a または 802.11b/g ネットワークにコールごとに必要な帯域幅を設定するには、**config 802.11 cac voice sip bandwidth** コマンドを使用します。

config 802.11 {**a** | **b**} **cac voice sip bandwidth** *bw_kbps* **sample-interval** *number_msecs*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
bw_kbps	帯域幅（kbps 単位）。
sample-interval	SIP コーデックのパケット化間隔を指定します。
number_msecs	ミリ秒単位のパケット化のサンプリング間隔。SIP コーデックのサンプリング間隔は 20 秒です。

コマンド デフォルト

なし

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable** ネットワーク コマンドを入力して、設定する無線ネットワークを無効にします。
- **save config** コマンドを入力して、新しい設定を保存します。
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、SIP コーデックの帯域幅と音声パケット化間隔を設定する例を示します。

```
(Cisco Controller) > config 802.11 cac voice sip bandwidth 10 sample-interval 40
```

関連コマンド

config 802.11 cac voice acm

config 802.11 cac voice load-based

config 802.11 cac voice max-bandwidth

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 exp-bwreq

config 802.11 cac voice sip codec

Call Admission Control（CAC）コーデック名とサンプル間隔をパラメータとして設定し、802.11a または 802.11b/g ネットワークに対するコールごとに必要な帯域幅を計算するには、**config 802.11 cac voice sip codec** コマンドを使用します。

config 802.11 {**a** | **b**} **cac voice sip codec** {**g711** | **g729**} **sample-interval** *number_msecs*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
g711	SIP G711 コーデックに CAC パラメータを指定します。
g729	SIP G729 コーデックに CAC パラメータを指定します。
sample-interval	SIP コーデックのパケット化間隔を指定します。
number_msecs	ミリ秒単位のパケット化間隔。SIP コーデック値のサンプリング間隔は 20 秒です。

コマンド デフォルト

デフォルトの CAC コーデック パラメータは g711 です。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable** ネットワーク コマンドを入力して、設定する無線ネットワークを無効にします。
- **save config** コマンドを入力して、新しい設定を保存します。
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、SIP G711 コーデックのパラメータとしてコーデック名とサンプリング間隔を設定する例を示します。

```
(Cisco Controller) >  config 802.11a cac voice sip codec g711 sample-interval 40
```

次に、SIP G729 コーデックのパラメータとしてコーデック名とサンプリング間隔を設定する例を示します。

```
(Cisco Controller) > config 802.11a cac voice sip codec g729 sample-interval 40
```

関連コマンド

config 802.11 cac voice acm

config 802.11 cac voice load-based

config 802.11 cac voice max-bandwidth

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 exp-bwreq

config 802.11 cac voice stream-size

802.11a または 802.11b/g ネットワーク用に指定されたデータ レートで集約音声 Wi-Fi マルチメディア（WMM）のトラフィック仕様（TSPEC）ストリーム数を設定するには、**config 802.11 cac voice stream-size** コマンドを使用します。

config 802.11 {**a** | **b**} **cac voice stream-size** *stream_size number* **mean_datarate max-streams** *mean_datarate*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
stream-size	ストリームの最大データ レートを設定します。
stream_size	ストリーム サイズの範囲は 84000 ～ 92100 です。
number	音声ストリームの数（1 ～ 5）。
mean_datarate	平均データ レートを設定します。
max-streams	音声ストリームの平均データ レートを設定します。
mean_datarate	音声ストリームの平均データ レート（84 ～ 91.2 Kbps）。

コマンド デフォルト

デフォルトのストリーム数は 2 で、ストリームの平均データ レートは 84 Kbps です。

使用上のガイドライン

コール アドミッション制御（CAC）コマンドでは、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **config wlan disable** *wlan_id* コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **config 802.11** {**a** | **b**} **disable** ネットワーク コマンドを入力して、設定する無線ネットワークを無効にします。
- **save config** コマンドを入力して、新しい設定を保存します。
- **config 802.11** {**a** | **b**} **cac voice acm enable** コマンドまたは **config 802.11** {**a** | **b**} **cac video acm enable** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ストリーム サイズ 5 および平均データ レート 85000 kbps の集約音声トラフィック仕様のストリームを設定する例を示します。

```
(Cisco Controller) > config 802.11 cac voice stream-size 5 max-streams size 85
```

関連コマンド

config 802.11 cac voice acm

config 802.11 cac voice load-based

config 802.11 cac voice max-bandwidth

config 802.11 cac voice roam-bandwidth

config 802.11 cac voice tspec-inactivity-timeout

config 802.11 exp-bwreq

config 802.11 cleanair

802.11a または 802.11b/g ネットワークに対して CleanAir を有効または無効にするには、**config 802.11 cleanair** コマンドを使用します。

config 802.11 {**a** | **b**} **cleanair** {**alarm** {**air-quality** {**disable** | **enable** | **threshold** *alarm_threshold* } | **device** {**disable** *device_type* | **enable** *device_type* | **reporting** {**disable** | **enable**} | **unclassified** {**disable** | **enable** | **threshold** *alarm_threshold* }} | **device** {**disable** *device_type* | **enable** *device_type* | **reporting** {**disable** | **enable**} | **disable** {**network** | *cisco_ap*} | **enable** {**network** | *cisco_ap*}}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
alarm	5 GHz cleanair アラームを設定します。
air-quality	5 GHz の電波品質のアラームを設定します。
enable	CleanAir の設定を有効にします。
disable	CleanAir の設定を無効にします。
threshold	5 GHz 電波品質のアラームしきい値を設定します。
alarm_threshold	電波品質のアラームしきい値（1=電波品質が悪い、100 = 電波品質がよい）。
device	5 GHz の CleanAir 干渉デバイスのアラームを設定します。

device_type	デバイス タイプ。デバイス タイプは次のとおりです。 • 802.11-nonstd：非標準の Wi-Fi チャネルを使用するデバイス。 • 802.11-inv：スペクトラム反転 Wi-Fi 信号を使用するデバイス。 • superag：802.11 SuperAG デバイス。 • all：すべての干渉デバイス タイプ。 • cont-tx：連続トランスミッタ。 • dect-like：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話。 • tdd-tx：TTY トランスミッタ。 • jammer：電波妨害装置。 • canopy：Canopy デバイス。 • video：ビデオ カメラ。 • wimax-mobile：WiMax モバイル。 • wimax-fixed：WiMax 固定。
reporting	5 GHz の CleanAir 干渉デバイスのアラーム レポートを設定します。
unclassified	分類されていないカテゴリの重大度を超えた場合の 5 GHz 電波品質のアラームを設定します。
network	5 GHz Cisco AP。
cisco_ap	このコマンドを適用するアクセス ポイントの名前。

コマンド デフォルト

802.11 a ネットワークまたは 802.11 b/g ネットワークの CleanAir 設定は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイント ap_24 の CleanAir 設定を有効にする例を示します。

```
(Cisco Controller) > config 802.11a cleanair enable ap_24
```

config 802.11 cleanair device

CleanAir 干渉デバイスのタイプを設定するには、**config 802.11 cleanair device** コマンドを使用します。

config 802.11{**a** | **b**} **cleanair device** {**enable** | **disable** | **reporting** {**enable** | **disable**}} *device_type*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	干渉デバイス タイプに対して CleanAir レポートを有効にします。
disable	干渉デバイス タイプに対して CleanAir レポートを無効にします。
reporting	CleanAir 干渉デバイスのレポートを設定します。
enable	5 GHz Cleanair の干渉デバイスのレポートを有効にします。
disable	5 GHz Cleanair の干渉デバイスのレポートを無効にします。

device_type	干渉デバイスのタイプ。デバイス タイプは次のとおりです。 • 802.11-nonstd：非標準の WiFi チャネルを使用するデバイス。 • 802.11-inv：スペクトラム反転 WiFi 信号を使用するデバイス。 • superag：802.11 SuperAG デバイス。 • all：すべての干渉デバイス タイプ。 • cont-tx：連続トランスミッタ。 • dect-like：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話。 • tdd-tx：TTY トランスミッタ。 • jammer：電波妨害装置。 • canopy：Canopy デバイス。 • video：ビデオ カメラ。 • wimax-mobile：WiMax モバイル。 • wimax-fixed：WiMax 固定。

コマンド デフォルト

干渉デバイス タイプの CleanAir レポートの設定は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、デバイス タイプ jammer の CleanAir レポートを有効にする例を示します。

```
(Cisco Controller) > config 802.11a cleanair device enable jammer
```

次に、デバイス タイプ video の CleanAir レポートを無効にする例を示します。

```
(Cisco Controller) > config 802.11a cleanair device disable video
```

次に、CleanAir 干渉デバイスのレポートを有効にする例を示します。

```
(Cisco Controller) > config 802.11a cleanair device reporting enable
```

config 802.11 cleanair alarm

電波品質アラームのトリガーを設定するには、**config 802.11 cleanair alarm** コマンドを使用します。

config 802.11 {**a** | **b**} **cleanair alarm** {**air-quality** {**disable** | **enable** | **threshold** *alarm_threshold* } | **device** {**disable** *device_type* | **enable** *device_type* | **reporting** {**disable** | **enable** } | **unclassified** {**disable** | **enable** | **threshold** *alarm_threshold* }}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
air-quality	5 GHz の電波品質のアラームを設定します。
disable	5 GHz 電波品質アラームを無効にします。
enable	5 GHz 電波品質のアラームを有効にします。
threshold	5 GHz 電波品質のアラームしきい値を設定します。
alarm_threshold	電波品質のアラームしきい値（1=電波品質が悪い、100 = 電波品質がよい）。
device	5 GHz の CleanAir 干渉デバイスのアラームを設定します。
all	すべてのデバイスタイプを一度に設定します。
reporting	5 GHz の CleanAir 干渉デバイスのアラーム レポートを設定します。
unclassified	分類されていないカテゴリの重大度を超えた場合の 5 GHz 電波品質のアラームを設定します。

device_type	デバイス タイプ。デバイス タイプは次のとおりです。 • 802.11-nonstd：非標準の Wi-Fi チャネルを使用するデバイス。 • 802.11-inv：スペクトラム反転 Wi-Fi 信号を使用するデバイス。 • superag：802.11 SuperAG デバイス。 • all：すべての干渉デバイス タイプ。 • cont-tx：連続トランスミッタ。 • dect-like：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話。 • tdd-tx：TTY トランスミッタ。 • jammer：電波妨害装置。 • canopy：Canopy デバイス。 • video：ビデオ カメラ。 • wimax-mobile：WiMax モバイル。 • wimax-fixed：WiMax 固定。

コマンド デフォルト

5 GHz 電波品質アラームの設定は、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、電波品質を監視する CleanAir アラームを有効にする例を示します。

```
(Cisco Controller) > config 802.11a cleanair alarm air-quality enable
```

次に、デバイス タイプ video の CleanAir アラームを有効にする例を示します。

```
(Cisco Controller) > config 802.11a cleanair alarm device enable video
```

次に、CleanAir 干渉デバイスのアラーム レポートを有効にする例を示します。

```
(Cisco Controller) > config 802.11a cleanair alarm device reporting enable
```

config 802.11 disable

802.11 ネットワーク全体または個々のシスコの無線に対して無線伝送を無効にするには、**config 802.11 disable** コマンドを使用します。

config 802.11 {**a** | **b**} **disable** {**network** | *cisco_ap* }

構文の説明

a	スロット 1 の 802.11a 無線とスロット 2 の 802.11ac 無線を設定します。
b	802.11b/g ネットワークを指定します。
network	802.11a ネットワーク全体で伝送を無効にします。
cisco_ap	個々の Cisco Lightweight アクセス ポイントの無線。

コマンド デフォルト

デフォルトでは、ネットワーク全体で伝送が有効化されています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

- さまざまな config 802.11 コマンドを使用する前に、次のコマンドを使用してネットワークを無効にする必要があります。
- このコマンドは、CLI インターフェイスがアクティブなときはいつでも使用できます。

次に、802.11a ネットワーク全体を無効にする例を示します。

```
(Cisco Controller) >config 802.11a disable network
```

次に、アクセス ポイント AP01 の 802.11b 伝送を無効にする例を示します。

```
(Cisco Controller) >config 802.11b disable AP01
```

config 802.11 dtpc

802.11 ネットワークの送信電力の動的制御（DTPC）設定を有効または無効にするには、**config 802.11 dtpc** コマンドを使用します。

config 802.11{**a** | **b**} **dtpc** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	このコマンドのサポートをイネーブルにします。
disable	このコマンドのサポートをディセーブルにします。

コマンド デフォルト

802.11 ネットワークの DTPC 設定は、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークの DTPC を無効にする例を示します。

```
(Cisco Controller) > config 802.11a dtpc disable
```

config 802.11 enable

802.11 ネットワーク全体または個々のシスコの無線に対して無線伝送を有効にするには、**config 802.11 enable** コマンドを使用します。

config 802.11{**a** | **b**} **enable** {**network** | *cisco_ap* }

構文の説明

a	スロット 1 の 802.11a 無線とスロット 2 の 802.11ac 無線を設定します。
b	802.11b/g ネットワークを指定します。
network	802.11a ネットワーク全体で伝送を無効にします。
cisco_ap	個々の Cisco Lightweight アクセス ポイントの無線。

コマンド デフォルト

デフォルトでは、ネットワーク全体で伝送が有効化されています。

使用上のガイドライン

802.11 を設定する場合は、このコマンドを **config 802.11 disable** コマンドとともに使用します。

このコマンドは、CLI インターフェイスがアクティブなときはいつでも使用できます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワーク全体の無線伝送を有効にする例を示します。

```
(Cisco Controller) > config 802.11a enable network
```

次に、802.11b ネットワークの API の無線伝送を有効にする例を示します。

```
(Cisco Controller) > config 802.11b enable AP1
```

関連コマンド

show sysinfo show 802.11a

config wlan radio

config 802.11a disable

config 802.11b disable

config 802.11b enable

config 802.11b 11gSupport enable

config 802.11b 11gSupport disable

config 802.11 exp-bwreq

802.11 無線の Cisco Client eXtension（CCX）v5 Expedited Bandwidth Request 機能を有効または無効にするには、**config 802.11 exp-bwreq** コマンドを使用します。

config 802.11{**a** | **b**} **exp-bwreq** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	Expedited Bandwidth Request 機能を有効にします。
disable	Expedited Bandwidth Request 機能を無効にします。

コマンド デフォルト

Expedited Bandwidth Request 機能はデフォルトでは無効になっています。

使用上のガイドライン

このコマンドが有効になっている場合、コントローラは結合されているすべてのアクセス ポイントでこの機能を設定します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CCX Expedited Bandwidth 設定を有効にする例を示します。

```
(Cisco Controller) > config 802.11a exp-bwreq enable
Cannot change Exp Bw Req mode while 802.11a network is operational.
```

次に、CCX Expedited Bandwidth 設定を無効にする例を示します。

```
(Cisco Controller) > config 802.11a exp-bwreq disable
```

関連コマンド

show 802.11a

show ap stats 802.11a

config 802.11 fragmentation

フラグメンテーションのしきい値を 802.11 ネットワークに設定するには、**config 802.11 fragmentation** コマンドを使用します。

config 802.11 {**a** | **b**} **fragmentation** *threshold*

（注） このコマンドは、**config 802.11 disable** コマンドでネットワークを無効にしてから使用します。

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
threshold	256 ～ 2346 バイトの数（両端の値を含む）。

コマンド デフォルト

なし。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークのフラグメンテーションしきい値を 6500 バイトのしきい値数で設定する例を示します。

```
(Cisco Controller) > config 802.11a fragmentation 6500
```

関連コマンド

config 802.11b fragmentation

show 802.11b

show ap auto-rtf

config 802.11 l2roam rf-params

802.11a または 802.11b/g レイヤ 2 クライアント ローミング パラメータを設定するには、**config 802.11 l2roam rf-params** コマンドを使用します。

config 802.11 {**a** | **b**} **l2roam rf-params** {**default** | **custom** *min_rssi roam_hyst scan_thresh trans_time*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
default	レイヤ 2 クライアントのローミング RF パラメータをデフォルト値に戻します。
custom	レイヤ 2 クライアントのカスタム ローミング RF パラメータを設定します。
min_rssi	クライアントをアクセス ポイントに関連付けるために必要な最小の受信信号強度インジケータ（RSSI）。クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。有効な範囲は -80 ～ -90 dBm で、デフォルト値は -85 dBm です。
roam_hyst	クライアントがローミングするために、周辺のアクセス ポイントの信号に必要な強度。このパラメータは、クライアントが 2 つのアクセス ポイント間のボーダー近くに物理的に存在している場合に、アクセスポイント間のローミングの量を減らすことを意図しています。有効な範囲は 2 ～ 4 dB で、デフォルト値は 2 dB です。

scan_thresh	許容可能な最小RSSI。この値を下回ると、クライアントはより適切なアクセス ポイントをローミングする必要があります。RSSIが指定された値より低い場合、クライアントは指定遷移時間内により強い信号のあるアクセス ポイントへローミングできる必要があります。このパラメータはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントはRSSIがしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。有効な範囲は -70 ～ -77 dBm で、デフォルト値は -72 dBm です。
trans_time	クライアントのアソシエートされたアクセス ポイントからのRSSIがスキャンのしきい値を下回った場合に、クライアントがローミングに適したネイバー アクセス ポイントの検出と、ローミングの完了にかけられる最大許容時間。有効な範囲は 1 ～ 10 秒で、デフォルト値は 5 秒です。 （注） 屋外メッシュ環境でのクライアントの高速ローミングに利用する場合には、遷移時間を 1 秒に設定することをお勧めします。

コマンド デフォルト

デフォルトの最小 RSSI は -85 dBm です。隣接するアクセス ポイントのデフォルトの信号強度は 2 dB です。デフォルトのスキャンしきい値は -72 dBm です。クライアントが適切な隣接アクセスポイントを検出してローミングし、ローミングを完了するために許容されるデフォルトの時間は 5 秒です。

使用上のガイドライン

屋外メッシュ環境でのクライアントの高速ローミングに利用する場合には、*trans_time* を 1 秒に設定することをお勧めします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a ネットワークにカスタム レイヤ 2 クライアント ローミング パラメータを設定する例を示します。

```
(Cisco Controller) > config 802.11 l2roam rf-params custom -80 2 -70 7
```

関連コマンド

show advanced 802.11 l2roam

show l2tp

config 802.11 max-clients

アクセス ポイントごとのクライアントの最大数を設定するには、**config 802.11 max-clients** コマンドを使用します。

config 802.11 {**a** | **b**} **max-clients** *max-clients*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
max-clients	アクセス ポイントごとのクライアント接続の最大数を設定します。
max-clients	アクセス ポイントごとのクライアント接続の最大数。指定できる範囲は 1 ～ 200 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントの最大数を 22 に設定する例を示します。

```
(Cisco Controller) > config 802.11 max-clients 22
```

関連コマンド

show ap config 802.11a

config 802.11b rate

config 802.11 media-stream multicast-direct

802.11 ネットワークのメディア ストリーム マルチキャスト ダイレクト パラメータを設定するには、**config 802.11 media-stream multicast-direct** コマンドを使用します。

config 802.11{**a** | **b**} **media-stream multicast-direct** {**admission-besteffort** {**enable** | **disable**} | {**client-maximum** | **radio-maximum**} {*value* | **no-limit** } | **enable** | **disable**}

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b/g ネットワークを指定します。
admission-besteffort	ベストエフォート キューにメディア ストリームを許可します。
enable	2.4 GHz または 5 GHz 帯域でマルチキャスト ダイレクトを有効にします。
disable	2.4 GHz または 5 GHz 帯域でマルチキャスト ダイレクトを無効にします。
client-maximum	クライアントで許可されるストリームの最大数を指定します。
radio-maximum	2.4 GHz または 5 GHz 帯域で許可されるストリームの最大数を指定します。
value	クライアント、または 2.4 GHz または 5 GHz 帯域で許可されるストリームの数（1～20）。
no-limit	クライアント、または 2.4 GHz または 5 GHz 帯域で許可されるストリームの数を無制限に指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

802.11 ネットワークのメディア ストリーム マルチキャスト ダイレクト パラメータを設定する前に、ネットワークが非動作であることを確認します。

次に、802.11a ネットワークでメディア ストリーム マルチキャスト ダイレクト設定を有効にする例を示します。

```
> config 802.11a media-stream multicast-direct enable
```

次に、ベスト エフォート キューにメディア ストリームを許可する例を示します。

```
> config 802.11a media-stream multicast-direct admission-besteffort enable
```

次に、クライアントで許可される最大ストリーム数を設定する例を示します。

```
> config 802.11a media-stream multicast-direct client-maximum 10
```

関連コマンド

config 802.11 media-stream video-redirect

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config 802.11 media-stream video-redirect

802.11 ネットワークのメディア ストリーム ビデオ リダイレクトを設定するには、**config 802.11 media-stream video-redirect** コマンドを使用します。

config 802.11 {**a** | **b**} **media-stream video-redirect** {**enable** | **disable**}

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b/g ネットワークを指定します。
enable	トラフィック リダイレクションを有効にします。
disable	トラフィック リダイレクションを無効にします。

コマンド デフォルト

なし。

使用上のガイドライン

802.11 ネットワークのメディア ストリーム ビデオ リダイレクションを設定する前に、ネットワークが非動作であることを確認します。

次に、802.11a ネットワークでメディア ストリーム トラフィック リダイレクションを有効にする例を示します。

```
> config 802.11a media-stream video-redirect enable
```

関連コマンド

config 802.11 media-stream multicast-redirect

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config 802.11 multicast data-rate

最小マルチキャスト データ レートを設定するには、**config 802.11 multicast data-rate** コマンドを使用します。

config 802.11{**a** | **b**} **multicast data-rate** *data_rate* [**ap** *ap_name* | **default**]

構文の説明

data_rate	最小のマルチキャスト データ レート。オプションは 6、9、12、18、24、36、48、54 です。APが、マルチキャストに割り当てられたバッファの数を動的に調整するように指定するには、0 を入力します。
ap_name	このデータ レートの特定の AP 無線。
default	このデータ レートですべての AP 無線を設定します。

コマンド デフォルト

デフォルトの0を設定すると、設定がディセーブルになります。マルチキャスト レートは最も低い必須データ レートおよびユニキャスト クライアント データ レートになります。

使用上のガイドライン

AP Name または **default** キーワードなしでデータ レートを設定すると、新しい値にすべてのAPがリセットされ、この新しいデータ レート値でコントローラのグローバル デフォルトが更新されます。**default** キーワードでデータ レートを設定すると、コントローラのグローバル デフォルト値のみが更新され、すでにコントローラを接続している AP の値はリセットされません。新しいデータ レート値を設定した後にコントローラに接続するAPは、新しいデータ レート値を受け取ります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、最小のマルチキャスト データ レートを設定する例を示します。

```
(Cisco Controller) > config 802.11 multicast data-rate 12
```

config 802.11 rate

802.11 ネットワークの必須およびサポート対象動作データ レートを設定するには、**config 802.11 rate** コマンドを使用します。

config 802.11 {**a** | **b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
disabled	特定のデータ レートをディセーブルにします。
mandatory	ネットワークを使用するためにクライアントがデータ レートをサポートするように指定します。
supported	ネットワークを使用するためにデータ レートをサポートする関連クライアントを許可するように指定します。
rate	6、9、12、18、24、36、48、または 54 Mbps のレート値。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドで設定したデータ レートは、クライアントと Cisco ワイヤレス LAN コントローラとの間でネゴシエートされます。データ レートが **mandatory** に設定されている場合、クライアントはネットワークを使用するためにこのデータ レートをサポートする必要があります。Cisco ワイヤレス LAN コントローラでデータ レートが **supported** に設定されている場合、アソシエートされているその他のクライアントのうち、このレートをサポートするクライアントも、このレートを使用して Cisco Lightweight アクセス ポイントと通信できます。アソシエートするために、クライアントが **supported** とマークされているすべてのレートを使用できる必要はありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、12 Mbps の必須レートで 802.11b 伝送を設定する例を示します。

```
(Cisco Controller) > config 802.11b rate mandatory 12
```

関連コマンド

show ap config 802.11a

config 802.11b rate

config 802.11 rssi-check

802.11 RSSI Low Check 機能を設定するには、**config 802.11 rssi-check** コマンドを使用します。

config 802.11 {**a**|**b**} **rssi-check** {**enable**|**disable**}

構文の説明

rssi-check	RSSI Low Check 機能を設定します。
enable	RSSI Low Check 機能を有効にします。
disable	RSSI Low Check 機能を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

config 802.11 rssi-threshold

802.11 RSSI Low Check しきい値を設定するには、**config 802.11 rssi-threshold** コマンドを使用します。

config 802.11{**a**|**b**} **rssi-threshold** *value-in-dBm*

構文の説明

rssi-threshold	RSSI Low Check しきい値を設定します。
value-in-dBm	RSSI しきい値（dBm 単位）。デフォルト値は -80 dBm です。

コマンド デフォルト

RSSI Low Check しきい値のデフォルト値は –80 dBm です。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

次に、802.11a ネットワークの RSSI しきい値を –70 dBm に設定する例を示します。

```
(Cisco Controller) > config 802.11a rssi-threshold -70
```

config 802.11 tsm

802.11a または 802.11b/g ネットワークに対するビデオ トラフィック ストリーム メトリック（TSM）オプションを有効または無効にするには、**config 802.11 tsm** コマンドを使用します。

config 802.11 {**a** | **b**} **tsm** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	ビデオ TSM 設定を有効にします。
disable	ビデオ TSM 設定をディセーブルにします。

コマンド デフォルト

802.11a ネットワークまたは 802.11b/g ネットワークの TSM は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11b/g ネットワークのビデオ TSM オプションを有効にする例を示します。

```
(Cisco Controller) > config 802.11b tsm enable
```

次に、802.11b/g ネットワークのビデオ TSM オプションを無効にする例を示します。

```
(Cisco Controller) > config 802.11b tsm disable
```

関連コマンド

show ap stats

show client tsm

config 802.11b preamble

サブクローズ 18.2.2.2 で定義されている 802.11b プリアンブルを **long**（遅いが信頼性が高い）または **short**（速いが信頼性が低い）に変更するには、**config 802.11b preamble** コマンドを使用します。

config 802.11b preamble {**long** | **short**}

構文の説明

long	long 802.11b プリアンブルを指定します。
short	short 802.11b プリアンブルを指定します。

コマンド デフォルト

802.11b プリアンブルのデフォルト値は short です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

（注） このコマンドを実装するには、保存して Cisco ワイヤレス LAN コントローラをリブート（システムをリセット）する必要があります。

SpectraLink 社の NetLink 電話など、一部のクライアント向けに Cisco ワイヤレス LAN コントローラを最適化するには、このパラメータを **long** に設定する必要があります。

このコマンドは、CLI インターフェイスがアクティブなときはいつでも使用できます。

次に、802.11b プリアンブルを short に変更する例を示します。

```
(Cisco Controller) >config 802.11b preamble short
(Cisco Controller) >(reset system with save)
```

config コマンド：a ～ i

- config aaa auth （183 ページ）
- config aaa auth mgmt （184 ページ）
- config acl apply （185 ページ）
- config acl counter （186 ページ）
- config acl create （187 ページ）
- config acl cpu （188 ページ）
- config acl delete （189 ページ）
- config acl layer2 （190 ページ）
- config acl rule （192 ページ）
- config acl url-domain （194 ページ）
- config advanced 802.11 7920VSIEConfig （195 ページ）
- config advanced 802.11 channel add （196 ページ）
- config advanced 802.11 channel cleanair-event （197 ページ）
- config advanced 802.11 channel dca anchor-time （198 ページ）
- config advanced 802.11 channel dca chan-width-11n （199 ページ）
- config advanced 802.11 channel dca interval （200 ページ）
- config advanced 802.11 channel dca min-metric （201 ページ）
- config advanced 802.11 channel dca sensitivity （202 ページ）
- config advanced 802.11 channel foreign （204 ページ）
- config advanced 802.11 channel load （205 ページ）
- config advanced 802.11 channel noise （206 ページ）
- config advanced 802.11 channel outdoor-ap-dca （207 ページ）
- config advanced 802.11 channel pda-prop （208 ページ）
- config advanced 802.11 channel update （209 ページ）
- config advanced 802.11 coverage （210 ページ）
- config advanced 802.11 coverage exception global （212 ページ）
- config advanced 802.11 coverage fail-rate （213 ページ）
- config advanced 802.11 coverage level global （215 ページ）
- config advanced 802.11 coverage packet-count （216 ページ）

- config advanced 802.11 coverage rssi-threshold （218 ページ）
- config advanced 802.11 edca-parameters （220 ページ）
- config advanced 802.11 factory （223 ページ）
- config advanced 802.11 group-member （224 ページ）
- config advanced 802.11 group-mode （225 ページ）
- config advanced 802.11 logging channel （226 ページ）
- config advanced 802.11 logging coverage （227 ページ）
- config advanced 802.11 logging foreign （228 ページ）
- config advanced 802.11 logging load （229 ページ）
- config advanced 802.11 logging noise （230 ページ）
- config advanced 802.11 logging performance （231 ページ）
- config advanced 802.11 logging txpower （232 ページ）
- config advanced 802.11 monitor channel-list （233 ページ）
- config advanced 802.11 monitor load （234 ページ）
- config advanced 802.11 monitor measurement （235 ページ）
- config advanced 802.11 monitor mode （236 ページ）
- config advanced 802.11 monitor ndp-type （237 ページ）
- config advanced 802.11 monitor timeout-factor （238 ページ）
- config advanced 802.11 optimized roaming （239 ページ）
- config advanced 802.11 packet （241 ページ）
- config advanced 802.11 profile clients （243 ページ）
- config advanced 802.11 profile customize （244 ページ）
- config advanced 802.11 profile foreign （245 ページ）
- config advanced 802.11 profile noise （246 ページ）
- config advanced 802.11 profile throughput （247 ページ）
- config advanced 802.11 profile utilization （248 ページ）
- config advanced 802.11 receiver （249 ページ）
- config advanced 802.11 reporting measurement （250 ページ）
- config advanced 802.11 tpc-version （251 ページ）
- config advanced 802.11 tpcv1-thresh （252 ページ）
- config advanced 802.11 tpcv2-intense （253 ページ）
- config advanced 802.11 tpcv2-per-chan （254 ページ）
- config advanced 802.11 tpcv2-thresh （255 ページ）
- config advanced 802.11 txpower-update （256 ページ）
- config advanced eap （257 ページ）
- config advanced hotspot （260 ページ）
- config advanced timers auth-timeout （262 ページ）
- config advanced timers eap-timeout （263 ページ）
- config advanced timers eap-identity-request-delay （264 ページ）
- config advanced timers （265 ページ）
- config advanced fastpath fastcache （268 ページ）

- config advanced fastpath pkt-capture （269 ページ）
- config advanced sip-preferred-call-no （270 ページ）
- config advanced sip-snooping-ports （271 ページ）
- config advanced backup-controller primary （272 ページ）
- config advanced backup-controller secondary （273 ページ）
- config advanced client-handoff （274 ページ）
- config advanced dot11-padding （275 ページ）
- config advanced assoc-limit （276 ページ）
- config advanced max-1x-sessions （277 ページ）
- config advanced rate （278 ページ）
- config advanced probe backoff （279 ページ）
- config advanced probe filter （280 ページ）
- config advanced probe limit （281 ページ）
- config advanced timers （282 ページ）
- config ap 802.1Xuser （285 ページ）
- config ap 802.1Xuser delete （286 ページ）
- config ap 802.1Xuser disable （287 ページ）
- config advanced dot11-padding （288 ページ）
- config ap （289 ページ）
- config ap aid-audit （290 ページ）
- config ap antenna band-mode （291 ページ）
- config ap atf 802.11 （292 ページ）
- config ap atf 802.11 policy （293 ページ）
- config ap autoconvert （294 ページ）
- config ap bhrate （295 ページ）
- config ap bridgegroupname （296 ページ）
- config ap bridging （297 ページ）
- config ap cdp （298 ページ）
- config ap core-dump （300 ページ）
- config ap crash-file clear-all （301 ページ）
- config ap crash-file delete （302 ページ）
- config ap crash-file get-crash-file （303 ページ）
- config ap crash-file get-radio-core-dump （304 ページ）
- config ap dtls-cipher-suite （305 ページ）
- config ap ethernet duplex （306 ページ）
- config ap ethernet tag （307 ページ）
- config ap autoconvert （308 ページ）
- config ap flexconnect bridge （309 ページ）
- config ap flexconnect central-dhcp （310 ページ）
- config ap flexconnect local-split （312 ページ）
- config ap flexconnect module-vlan （313 ページ）

- config ap flexconnect policy （314 ページ）
- config ap flexconnect radius auth set （315 ページ）
- config ap flexconnect vlan （316 ページ）
- config ap flexconnect vlan add （317 ページ）
- config ap flexconnect vlan native （318 ページ）
- config ap flexconnect vlan wlan （319 ページ）
- config ap flexconnect web-auth （320 ページ）
- config ap flexconnect web-policy acl （321 ページ）
- config ap flexconnect wlan （322 ページ）
- config ap group-name （323 ページ）
- config ap hotspot （324 ページ）
- config ap image predownload （331 ページ）
- config ap image swap （332 ページ）
- config ap lag-mode support （333 ページ）
- config ap led-state （334 ページ）
- config ap link-encryption （335 ページ）
- config ap link-latency （336 ページ）
- config ap location （337 ページ）
- config ap logging syslog level （338 ページ）
- config ap logging syslog facility （339 ページ）
- config ap max-count （342 ページ）
- config ap mgmtuser add （343 ページ）
- config ap mgmtuser delete （345 ページ）
- config ap mode （346 ページ）
- config ap module3g （348 ページ）
- config ap monitor-mode （349 ページ）
- config ap name （350 ページ）
- config ap packet-dump （351 ページ）
- config ap port （355 ページ）
- config ap power injector （356 ページ）
- config ap power pre-standard （357 ページ）
- config ap preferred-mode （358 ページ）
- config ap primary-base （359 ページ）
- config ap priority （361 ページ）
- config ap reporting-period （362 ページ）
- config ap reset （363 ページ）
- config ap retransmit interval （364 ページ）
- config ap retransmit count （365 ページ）
- config ap role （366 ページ）
- config ap rst-button （367 ページ）
- config ap secondary-base （368 ページ）

- config ap slub-debug （370 ページ）
- config ap sniff （372 ページ）
- config ap ssh （374 ページ）
- config ap static-ip （375 ページ）
- config ap stats-timer （377 ページ）
- config ap syslog host global （378 ページ）
- config ap syslog host specific （379 ページ）
- config ap tcp-mss-adjust （380 ページ）
- config ap telnet （381 ページ）
- config ap tertiary-base （382 ページ）
- config ap tftp-downgrade （384 ページ）
- config ap username （385 ページ）
- config ap venue （386 ページ）
- config ap wlan （390 ページ）
- config atf 802.11 （391 ページ）
- config atf policy （392 ページ）
- config auth-list add （393 ページ）
- config auth-list ap-policy （394 ページ）
- config auth-list delete （395 ページ）
- config avc profile create （396 ページ）
- config avc profile delete （397 ページ）
- config avc profile rule （398 ページ）
- config band-select cycle-count （400 ページ）
- config band-select cycle-threshold （401 ページ）
- config band-select expire （402 ページ）
- config band-select client-rssi （403 ページ）
- config boot （404 ページ）
- config call-home contact email address （405 ページ）
- config call-home events （406 ページ）
- config call-home http-proxy ipaddr （407 ページ）
- config call-home http-proxy ipaddr 0.0.0.0 （408 ページ）
- config call-home profile （409 ページ）
- config call-home profile delete （410 ページ）
- config call-home profile status （411 ページ）
- config call-home reporting （412 ページ）
- config call-home tac-profile （413 ページ）
- config cdp （414 ページ）
- config certificate lsc （415 ページ）
- config certificate ssc （418 ページ）
- config certificate use-device-certificate webadmin （420 ページ）
- config client ccx clear-reports （421 ページ）

- config client ccx clear-results （422 ページ）
- config client ccx default-gw-ping （423 ページ）
- config client ccx dhcp-test （424 ページ）
- config client ccx dns-ping （425 ページ）
- config client ccx dns-resolve （426 ページ）
- config client ccx get-client-capability （427 ページ）
- config client ccx get-manufacturer-info （428 ページ）
- config client ccx get-operating-parameters （429 ページ）
- config client ccx get-profiles （430 ページ）
- config client ccx log-request （431 ページ）
- config client ccx send-message （433 ページ）
- config client ccx stats-request （437 ページ）
- config client ccx test-abort （438 ページ）
- config client ccx test-association （439 ページ）
- config client ccx test-dot1x （440 ページ）
- config client ccx test-profile （441 ページ）
- config client deauthenticate （442 ページ）
- config client location-calibration （443 ページ）
- config client profiling delete （444 ページ）
- config coredump （445 ページ）
- config coredump ftp （446 ページ）
- config coredump username （447 ページ）
- config country （448 ページ）
- config cts sxp （449 ページ）
- config custom-web ext-webauth-mode （451 ページ）
- config custom-web ext-webauth-url （452 ページ）
- config custom-web ext-webserver （453 ページ）
- config custom-web logout-popup （454 ページ）
- config custom-web radiusauth （455 ページ）
- config custom-web redirectUrl （456 ページ）
- config custom-web sleep-client （457 ページ）
- config custom-web webauth-type （458 ページ）
- config custom-web weblogo （459 ページ）
- config custom-web webmessage （460 ページ）
- config custom-web webtitle （461 ページ）
- config database size （462 ページ）
- config dhcp （463 ページ）
- config dhcp opt-82 format （466 ページ）
- config dhcp opt-82 remote-id （467 ページ）
- config dhcp proxy （469 ページ）
- config dhcp timeout （470 ページ）

- config exclusionlist （471 ページ）
- config flexconnect [ipv6] acl （472 ページ）
- config flexconnect [ipv6] acl rule （473 ページ）
- config flexconnect [ipv6] acl url-domain （475 ページ）
- config flexconnect arp-caching （476 ページ）
- config flexconnect avc profile （477 ページ）
- config flexconnect fallback-radio-shut （478 ページ）
- config flexconnect group （479 ページ）
- config flexconnect group vlan （485 ページ）
- config flexconnect group *group-name* dhcp overridden-interface （486 ページ）
- config flexconnect group web-auth （487 ページ）
- config flexconnect group web-policy （488 ページ）
- config flexconnect join min-latency （489 ページ）
- config flexconnect office-extend （490 ページ）
- config flow （492 ページ）
- config guest-lan （493 ページ）
- config guest-lan custom-web ext-webauth-url （494 ページ）
- config guest-lan custom-web global disable （495 ページ）
- config guest-lan custom-web login_page （496 ページ）
- config guest-lan custom-web webauth-type （497 ページ）
- config guest-lan ingress-interface （498 ページ）
- config guest-lan interface （499 ページ）
- config guest-lan mobility anchor （500 ページ）
- config guest-lan nac （501 ページ）
- config guest-lan security （502 ページ）
- config interface 3g-vlan （503 ページ）
- config interface acl （504 ページ）
- config interface address （505 ページ）
- config interface address redundancy-management （507 ページ）
- config interface ap-manager （508 ページ）
- config interface create （509 ページ）
- config interface delete （510 ページ）
- config interface dhcp management （511 ページ）
- config interface dhcp （513 ページ）
- config interface address （514 ページ）
- config interface guest-lan （516 ページ）
- config interface hostname （517 ページ）
- config interface nasid （518 ページ）
- config interface nat-address （519 ページ）
- config interface port （520 ページ）
- config interface quarantine vlan （521 ページ）

- config interface vlan （522 ページ）
- config interface group mdns-profile （523 ページ）
- config interface mdns-profile （525 ページ）
- config icons delete （527 ページ）
- config icons file-info （528 ページ）
- config ipv6 disable （529 ページ）
- config ipv6 enable （530 ページ）
- config ipv6 acl （531 ページ）
- config ipv6 capwap （533 ページ）
- config ipv6 interface （534 ページ）
- config ipv6 interface multicast （536 ページ）
- config ipv6 neighbor-binding （537 ページ）
- config ipv6 na-mcast-fwd （539 ページ）
- config ipv6 ns-mcast-fwd （540 ページ）
- config ipv6 ra-guard （541 ページ）
- config ipv6 route （542 ページ）

config aaa auth

管理ユーザに対する AAA 認証の検索順序を設定するには、**config aaa auth** コマンドを使用します。

config aaa auth mgmt [*aaa_server_type1* | *aaa_server_type2*]

構文の説明

mgmt	最大 3 つの AAA 認証サーバ タイプを指定して、コントローラの管理ユーザに対する AAA 認証の検索順序を設定します。サーバ タイプの入力順序により AAA 認証の検索順序が指定されます。
aaa_server_type	（任意）AAA 認証サーバのタイプ（**local**、**radius**、または **tacacs**）。**local** 設定ではローカル データベース、**radius** 設定では RADIUS サーバ、**tacacs** 設定では TACACS+ サーバが指定されます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

AAA サーバ タイプは、片方が **local** ならば 2 つ入力できます。**radius** と **tacacs** をいっしょに入力することはできません。

次に、local の認証サーバ タイプによってコントローラの管理ユーザに対する AAA 認証の検索順序を設定する例を示します。

```
(Cisco Controller) > config aaa auth radius local
```

関連コマンド

show aaa auth

config aaa auth mgmt

複数データベースが設定されている場合に認証の順序を設定するには、**config aaa auth mgmt** コマンドを使用します。

config aaa auth mgmt［**radius** | **tacacs**］

構文の説明

radius	（任意）RADIUS サーバに認証の順序を設定します。
tacacs	（任意）TACACS サーバに認証の順序を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、RADIUS サーバに認証の順序を設定する例を示します。

```
(Cisco Controller) > config aaa auth mgmt radius
```

次に、TACACS サーバに認証の順序を設定する例を示します。

```
(Cisco Controller) > config aaa auth mgmt tacacs
```

関連コマンド

show aaa auth order

config acl apply

アクセス コントロール リスト（ACL）をデータ パスに適用するには、**config acl apply** コマンドを使用します。

config acl apply *rule_name*

構文の説明

rule_name	最大 32 文字の英数字による ACL 名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、ACL をデータ パスに適用する例を示します。

```
(Cisco Controller) > config acl apply acl01
```

関連コマンド

show acl

config acl counter

パケットが、コントローラ上に設定されたアクセス コントロール リスト（ACL）のいずれかをヒットしたかどうかを確認するには、**config acl counter** コマンドを使用します。

config acl counter {**start** | **stop**}

構文の説明

start	コントローラで ACL カウンタを有効にします。
stop	コントローラで ACL カウンタを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ACL カウンタを使用できるコントローラは、4400 シリーズ、Cisco WiSM、Catalyst 3750G Integrated Wireless LAN Controller Switch だけです。

次に、コントローラで ACL カウンタを有効にする例を示します。

```
(Cisco Controller) > config acl counter start
```

関連コマンド

clear acl counters

show acl detailed

config acl create

新しいアクセス コントロール リスト（ACL）を作成するには、**config acl create** コマンドを使用します。

config acl create *rule_name*

構文の説明

rule_name	最大 32 文字の英数字による ACL 名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、新しい ACL を作成する例を示します。

```
(Cisco Controller) > config acl create acl01
```

関連コマンド

show acl

config acl cpu

CPU に到達するトラフィックを制限する新しいアクセス コントロール リスト（ACL）を作成するには、**config acl cpu** コマンドを使用します。

config acl cpu *rule_name* {**wired** | **wireless** | **both**}

構文の説明

rule_name	ACL 名を指定します。
wired	有線トラフィックで ACL を指定します。
wireless	無線トラフィックで ACL を指定します。
both	有線と無線両方のトラフィックで ACL を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、CPU に到達するパケットのタイプを制御できます。

次に、CPU で acl101 という ACL を作成し、有線トラフィックに適用する例を示します。

```
(Cisco Controller) > config acl cpu acl01 wired
```

関連コマンド

show acl cpu

config acl delete

アクセス コントロール リスト（ACL）を削除するには、**config acl delete** コマンドを使用します。

config acl delete *rule_name*

構文の説明

rule_name	最大 32 文字の英数字による ACL 名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、CPU で acl101 という ACL を削除する例を示します。

```
(Cisco Controller) > config acl delete acl01
```

関連コマンド

show acl

config acl layer2

レイヤ 2 アクセス コントロール リスト（ACL）を設定するには、**config acl layer2** コマンドを使用します。

config acl layer2 {**apply** *acl_name* | **create** *acl_name* | **delete** *acl_name* | **rule** {**action** *acl_name index* {**permit** | **deny**} | **add** *acl_name index* | **change index** *acl_name old_index new_index* | **delete** *acl_name index* | **etherType** *acl_name index etherType etherTypeMask* | **swap index** *acl_name index1 index2*}}

構文の説明

apply	レイヤ 2 ACL をデータ パスに適用します。
acl_name	レイヤ 2 ACL の名前。名前には 32 文字以内の英数字を使用できます。
create	レイヤ 2 ACL を作成します。
delete	レイヤ 2 ACL を削除します。
rule	レイヤ 2 ACL ルールを設定します。
action	レイヤ 2 ACL ルールのアクションを設定します。
index	レイヤ 2 ACL ルールのインデックス。
permit	ルールのアクションを許可します。
deny	ルールのアクションを拒否します。
add	レイヤ 2 ACL ルールを作成します。
change index	レイヤ 2 ACL ルールのインデックスを変更します。
old_index	レイヤ 2 ACL ルールの古いインデックス。
new_index	レイヤ 2 ACL ルールの新しいインデックス。
delete	レイヤ 2 ACL ルールを削除します。
etherType	レイヤ 2 ACLルールの EtherType を設定します。
etherType	レイヤ 2 ACLルールの EtherType。EtherType は、イーサネット フレームのペイロードにカプセル化されるプロトコルを示すために使用されます。範囲は 16 進値の 0x0 ～ 0xffff です。

etherTypeMask	EtherType のネットマスク。範囲は 16 進値の 0x0 ～ 0xffff です。
swap index	2つのルールのインデックス値を交換します。
index1 index2	2つのレイヤ2 ACL ルールのインデックス値。

コマンド デフォルト

Cisco WLC はレイヤ 2 ACL を持っていません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 ACL に対して最大 16 のルールを作成できます。

Cisco WLC には、最大で 64 の レイヤ 2 ACL を作成できます。

アクセス ポイントは最大 16 の WLAN をサポートするので、アクセス ポイントごとに最大 16 のレイヤ 2 ACL がサポートされます。

アクセス ポイントはレイヤ 2 およびレイヤ 3 の同じ ACL 名をサポートしないため、レイヤ 2 ACL 名が FlexConnect ACL 名と競合していないことを確認します。

次に、レイヤ 2 ACL を適用する例を示します。

```
(Cisco Controller) >config acl layer2 apply acl_l2_1
```

config acl rule

ACL ルールを設定するには、**config acl rule** コマンドを使用します。

config acl rule {**action** *rule_name rule_index* {**permit** | **deny**} | **add** *rule_name rule_index* | **change index** *rule_name old_index new_index* | **delete** *rule_name rule_index* | **destination address** *rule_name rule_index ip_address netmask* | **destination port range** *rule_name rule_index start_port end_port* | **direction** *rule_name rule_index* {**in** | **out** | **any**} | **dscp** *rule_name rule_index dscp* | **protocol** *rule_name rule_index protocol* | **source address** *rule_name rule_index ip_address netmask* | **source port range** *rule_name rule_index start_port end_port* | **swap index** *rule_name index_1 index_2*}

構文の説明

action	アクセスを許可するか拒否するかを設定します。
rule_name	最大 32 文字の英数字による ACL 名。
rule_index	1 ～ 32 のルールのインデックス。
permit	ルールのアクションを許可します。
deny	ルールのアクションを拒否します。
add	新規ルールを追加します。
change	ルールのインデックスを変更します。
index	ルールのインデックスを指定します。
delete	ルールを削除します。
destination address	ルールの宛先 IP アドレスとネットマスクを設定します。
destination port range	ルールの宛先ポート範囲を設定します。
ip_address	ルールの IP アドレス。
netmask	ルールのネットマスク。
start_port	開始ポート番号（0 ～ 65535）。
end_port	終了ポート番号（0 ～ 65535）。
direction	ルールの方向（in、out、または any）を設定します。
in	ルールの方向を in に設定します。
out	ルールの方向を out に設定します。

any	ルールの方向を any に設定します。
dscp	ルールの DSCP を設定します。
dscp	0 ～ 63 の数値または **any**。
protocol	ルールの DSCP を設定します。
protocol	0 ～ 255 の数値または **any**。
source address	ルールの送信元 IP アドレスとネットマスクを設定します。
source port range	ルールの送信元ポート範囲を設定します。
swap	ルールの2つのインデックスを入れ替えます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web Policy で無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、アクセスを許可するよう ACL を設定する例を示します。

```
(Cisco Controller) > config acl rule action lab1 4 permit
```

関連コマンド

show acl

config acl url-domain

アクセス コントロール リストのURL ドメインを追加または削除するには、**config acl url-domain** コマンドを使用します。

config acl url-domain{**add**|**delete**} *domain_name acl_name*

構文の説明

domain_name	アクセス コントロール リストの URL ドメイン名。
acl_name	アクセス コントロール リストの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。

次に、アクセス コントロール リストの新しいURL ドメインを追加する例を示します。

```
(Cisco Controller) > config acl url-domain add cisco.com android
```

次に、アクセス コントロール リストから既存の URL ドメインを削除する例を示します。

```
(Cisco Controller) > config acl url-domain delete play.google.com android
```

config advanced 802.11 7920VSIEConfig

Cisco Unified Wireless IP Phone 7920 VISE パラメータを設定するには、**config advanced 802.11 7920VSIEConfig** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **7920VSIEConfig** {**call-admission-limit** *limit* | **G711-CU-Quantum** *quantum*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
call-admission-limit	7920s のコール アドミッション制限を設定します。
G711-CU-Quantum	単一の G.711-20ms コールで使用されるチャネル使用率の単位の現在の数を示すインフラストラクチャによって提供される値を設定します。
limit	コール アドミッション制限（0 ～ 255）。デフォルト値は 105 です。
quantum	G711 量子値。デフォルト値は 15 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、7920 VISE パラメータのコール アドミッション制限を設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 7920VSIEConfig call-admission-limit 4
```

config advanced 802.11 channel add

802.11 ネットワーク自動 RF チャネルのリストにチャネルを追加するには、**config advanced 802.11 channel add** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel add** *channel_number*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
add	802.11 ネットワーク自動 RF チャネルのリストにチャネルを追加します。
channel_number	802.11 ネットワーク自動 RF チャネルのリストに追加するチャネル番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワーク自動 RF チャネルのリストにチャネルを追加する例を示します。

```
(Cisco Controller) >config advanced 802.11 channel add 132
```

config advanced 802.11 channel cleanair-event

すべての 802.11 Cisco Lightweight アクセス ポイントの CleanAir イベント駆動型無線リソース管理（RRM）パラメータを設定するには、**config advanced 802.11 channel cleanair-event** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel cleanair-event** {**enable** | **disable** | **sensitivity** [**low** | **medium** | **high**] | **custom threshold** *threshold_value*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	CleanAir イベント駆動型 RRM パラメータを有効にします。
disable	CleanAir イベント駆動型 RRM パラメータを無効にします。
sensitivity	CleanAir イベント駆動型 RRM の感度を設定します。
low	（任意）低感度を指定します。
medium	（任意）中感度を指定します。
high	（任意）高感度を指定します。
custom	カスタム感度を指定します。
threshold	EDRRM AQ しきい値を指定します。
threshold_value	カスタムしきい値の数。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CleanAir イベント駆動 RRM パラメータを有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 channel cleanair-event enable
```

次に、CleanAir イベント駆動型 RRM に高感度を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 channel cleanair-event sensitivity high
```

config advanced 802.11 channel dca anchor-time

チャネルの動的割り当て（DCA）アルゴリズムの開始時刻を指定するには、 **config advanced 802.11 channel dca anchor-time** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dca anchor-time** *value*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
value	0 ～ 23 の時刻。この値は、午前 12 時から午後 11 時までの時間を表します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、DCA アルゴリズムが開始したときに遅延時間を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 channel dca anchor-time 17
```

関連コマンド

config advanced 802.11 channel dca interval

config advanced 802.11 channel dca sensitivity

config advanced 802.11 channel

config advanced 802.11 channel dca chan-width-11n

5 GHz 帯域のすべての 802.11n 無線に、チャネルの動的割り当て（DCA）チャネル幅を設定するには、**config advanced 802.11 channel dca chan-width-11n** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dca chan-width-11n** {**20** | **40** | **80**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
20	802.11n 無線のチャネル幅を 20 MHz に設定します。
40	802.11n 無線のチャネル幅を 40 MHz に設定します。
80	802.11ac 無線のチャネル幅を 80 MHz に設定します。

コマンド デフォルト

デフォルトのチャネル幅は 20 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

40 を選択する場合は、 **config advanced 802.11 channel** {**add** | **delete**} *channel_number* コマンドで少なくとも 2 つの隣接チャネルを設定する必要があります（プライマリ チャネルの 36 と拡張チャネルの 40 など）。1 つのチャネルしか設定しないと、そのチャネルは 40 MHz チャネル幅として使用されません。

グローバルに設定されている DCA チャネル幅設定を上書きするには、**config 802.11 chan_width** コマンドを使用して、特定のアクセス ポイントの無線を 20 または 40 MHz モードに静的に設定します。後でこのアクセスポイントの無線に対する静的な設定をグローバルに変更すると、それまでアクセス ポイントで使用されていたチャネル幅設定はグローバルな DCA 設定で上書きされます。

次に、802.11a ネットワーク自動チャネルのリストにチャネルを追加する例を示します。

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 40
```

次に、802.11ac 無線のチャネル幅を 80 MHz に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 80
```

config advanced 802.11 channel dca interval

チャネルの動的割り当て（DCA）が実行される頻度を指定するには、 **config advanced 802.11 channel dca interval** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dca interval** *value*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
value	有効な値は0、1、2、3、4、6、8、12、または24時間です。0の場合は10分になります（600秒）。

コマンド デフォルト

DCA チャネルのデフォルトの間隔は 10（10 分）です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

コントローラがOfficeExtendアクセスポイントしかサポートしていない場合は、最適なパフォーマンスを得るために、DCA 間隔を 6 時間に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントを組み合わせて展開している場合は、10 分から 24 時間までの範囲を使用できます。

次に、DCA アルゴリズムが実行される頻度の例を示します。

```
(Cisco Controller) > config advanced 802.11 channel dca interval 8
```

関連コマンド

config advanced 802.11 dca anchor-time

config advanced 802.11 dca sensitivity

show advanced 802.11 channel

config advanced 802.11 channel dca min-metric

DCA の 5 GHz 最小 RSSI エネルギー メトリックを設定するには、**config advanced 802.11 channel dca min-metric** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dca** *RSSI_value*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
RSSI_value	DCA がチャネルの変更をトリガーするために必要な最小の受信信号強度インジケータ（RSSI）。範囲は、-100 ～ -60 dBm です。

コマンド デフォルト

DCA のデフォルトの最小 RSSI エネルギー メトリックは、–95 dBm です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、DCA の 5 GHz 最小 RSSI エネルギー メトリックを設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a channel dca min-metric –80
```

上記の例では、DCA がチャネルの変更をトリガーするために、RSSI で少なくとも -80 dBm の干渉エネルギーを RRM が検出する必要があります。

関連コマンド

config advanced 802.11 dca interval

config advanced 802.11 dca anchor-time

show advanced 802.11 channel

config advanced 802.11 channel dca sensitivity

チャネル変更の判定時の環境の変化（信号、負荷、ノイズ、干渉など）に対するチャネルの動的割り当て（DCA）アルゴリズムの感度を指定するには、**config advanced 802.11 channel dca sensitivity** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dcasensitivity** {**low** | **medium** | **high**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
low	環境の変化に対する DCA アルゴリズムの感度は特に高くないことを指定します。詳細については、「使用上のガイドライン」を参照してください。
medium	環境の変化に対する DCA アルゴリズムの感度は中程度であることを指定します。詳細については、「使用上のガイドライン」を参照してください。
high	環境の変化に対する DCA アルゴリズムの感度が高いことを指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

トラブルシューティングに役立つように、このコマンドの出力には失敗したコールすべてのエラー コードが示されます。次の表では、失敗したコールの考えられるエラー コードについて説明します。

表 *4: DCA* の感度のしきい値

感度	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
High	5 dB	5 dB
Medium	15 dB	20 dB

感度	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
Low	30 dB	35 dB

次に、DCA アルゴリズムの感度の値を low に設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 channel dca sensitivity low
```

関連コマンド

config advanced 802.11 dca interval

config advanced 802.11 dca anchor-time

show advanced 802.11 channel

config advanced 802.11 channel foreign

802.11a対応のすべてのCisco Lightweightアクセス ポイントについて、無線リソース管理（RRM）によるチャネル選択時に外部 802.11a 干渉回避を考慮するか、無視するかを指定するには、**config advanced 802.11 channel foreign** コマンドを使用します。

config advanced 802.11{**a** | **b**} **channel foreign** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	チャネル割り当てで、外部アクセス ポイント 802.11a 干渉回避を有効にします。
disable	チャネル割り当てで、外部アクセス ポイント 802.11a 干渉回避を無効にします。

コマンド デフォルト

チャネル割り当てでの外部アクセス ポイント 802.11a 干渉回避は、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a 対応のすべての Cisco Lightweight アクセス ポイントについて、RRM によるチャネル選択時に外部 802.11a 干渉が考慮されるようにする例を示します。

```
(Cisco Controller) > config advanced 802.11a channel foreign enable
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11b channel foreign

config advanced 802.11 channel load

802.11a 対応のすべての Cisco Lightweight アクセス ポイントについて、無線リソース管理（RRM）によるチャネル選択更新時にトラフィックの負荷を考慮するか、無視するかを指定するには、**config advanced 802.11 channel load** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel load** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	チャネル割り当てで、Cisco Lightweight アクセス ポイント 802.11a 負荷回避を有効にします。
disable	チャネル割り当てで、Cisco Lightweight アクセス ポイント 802.11a 負荷回避を無効にします。

コマンド デフォルト

チャネル割り当てでの Cisco Lightweight アクセス ポイント 802.11a 負荷回避は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a 対応のすべての Cisco Lightweight アクセス ポイントについて、RRM によるチャネル選択時にトラフィックの負荷が考慮されるようにする例を示します。

```
(Cisco Controller) > config advanced 802.11 channel load enable
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11b channel load

config advanced 802.11 channel noise

802.11a対応のすべてのCisco Lightweightアクセス ポイントについて、無線リソース管理（RRM）によるチャネル選択更新時に802.11a以外のノイズを考慮するか、無視するかを指定するには、**config advanced 802.11 channel noise** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel noise** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	チャネル割り当てで802.11a以外のノイズ回避を有効にするか、無視します。
disable	チャネル割り当てで802.11a以外のノイズ回避を無効にします。

コマンド デフォルト

チャネル割り当てで 802.11a 以外のノイズ回避は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a 対応のすべての Cisco Lightweight アクセス ポイントについて、RRM によるチャネル選択時に 802.11a 以外のノイズが考慮されるようにする例を示します。

```
(Cisco Controller) > config advanced 802.11 channel noise enable
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11b channel noise

config advanced 802.11 channel outdoor-ap-dca

非動的周波数選択（DFS）チャネルのチェックのコントローラによる回避を有効または無効にするには、**config advanced 802.11 channel outdoor-ap-dca** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel outdoor-ap-dca** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションを有効にします。
disable	屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションを無効にします。

コマンド デフォルト

屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config advanced 802.11 {**a** | **b**} **channel outdoor-ap-dca** {**enable** | **disable**} コマンドは、1522 や 1524 などの屋外アクセス ポイントを持つ展開にのみ適用されます。

次に、屋外アクセス ポイントで 802.11a DCA のリスト オプションを有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11a channel outdoor-ap-dca enable
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11b channel noise

config advanced 802.11 channel pda-prop

永続デバイスの伝播を有効または無効にするには、**config advanced 802.11 channel pda-prop** コマンドを使用します。

config advanced 802.11{**a** | **b**} **channel pda-prop** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションを有効にします。
disable	屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションを無効にします。

コマンド デフォルト

屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、永続デバイスの伝播を有効または無効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 channel pda-prop enable
```

config advanced 802.11 channel update

802.11a 対応のすべての Cisco Lightweight アクセス ポイントを対象に、無線リソース管理（RRM）によるチャネル選択更新が開始されるようにするには、**config advanced 802.11 channel update** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel update**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての 802.11a ネットワーク アクセス ポイントのチャネル選択の更新を開始する例を示します。

```
(Cisco Controller) > config advanced 802.11a channel update
```

config advanced 802.11 coverage

カバレッジ ホール検出を有効または無効にするには、**config advanced 802.11 coverage** コマンドを使用します。

config advanced 802.11{**a** | **b**} **coverage** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	カバレッジ ホールの検出を有効にします。
disable	カバレッジ ホールの検出を無効にします。

コマンド デフォルト

カバレッジ ホール検出は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

カバレッジホール検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいて Cisco WLC が自動的に判断します。

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global**コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。Cisco WLC は、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、802.11aネットワーク上でカバレッジホールの検出を有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11a coverage enable
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage exception global

アクセス ポイント上で、信号レベルが低くなっているにもかかわらず、別のアクセス ポイントにローミングできないクライアントの割合を指定するには、**config advanced 802.11 coverage exception global** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **coverage exception global** *percent*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
percent	クライアントの割合。有効な値は 0 ～ 100 % です。

コマンド デフォルト

アクセス ポイントでのクライアントの割合は、デフォルトでは 25 % です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global** コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、信号レベルが低くなっているすべての 802.11a アクセス ポイントにクライアントの割合を指定する例を示します。

```
(Cisco Controller) > config advanced 802.11 coverage exception global 50
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

config advanced 802.11 coverage fail-rate

アップリンクのデータ パケットまたは音声パケットの失敗率のしきい値を指定するには、**config advanced 802.11 coverage fail-rate** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **coverage** {**data** | **voice**} **fail-rate** *percent*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
data	データ パケットのしきい値を指定します。
voice	音声パケットのしきい値を指定します。
percent	失敗率のパーセント。有効な値は 1 ～ 100 % です。

コマンド デフォルト

アップリンク カバレッジ失敗率値のデフォルトの失敗率しきい値は、20 % です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global**コマンドおよび**config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、データ パケットの最小アップリンク失敗率のしきい値を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 coverage fail-rate 80
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

config advanced 802.11 coverage level global

アクセス ポイント上でデータまたは音声受信信号強度インジケータ（RSSI）しきい値以下の RSSI 値を持つクライアントの最小数を指定するには、**config advanced 802.11 coverage level global** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **coverage level global** *clients*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
clients	クライアントの最小数。有効な値は 1 ～ 75 です。

コマンド デフォルト

アクセス ポイント上のクライアントのデフォルトの最小数は 3 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global**コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、RSSI しきい値以下の RSSI 値をすべての 802.11a アクセス ポイントでクライアントの最小数を指定する例を示します。

```
(Cisco Controller) > config advanced 802.11 coverage level global 60
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

config advanced 802.11 coverage packet-count

アップリンクのデータ パケットまたは音声パケットの最小失敗数のしきい値を指定するには、**config advanced 802.11 coverage packet-count** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **coverage** {**data** | **voice**} **packet-count** *packets*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
data	データ パケットのしきい値を指定します。
voice	音声パケットのしきい値を指定します。
packets	パケットの最小数。有効な値は 1 ～ 255 パケットです。

コマンド デフォルト

アップリンク データまたは音声パケットのデフォルトの失敗カウントしきい値は 10 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global**コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、アップリンク データ パケットに対して失敗数のしきい値を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 coverage packet-count 100
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

config advanced 802.11 coverage rssi-threshold

アクセス ポイントで受信されるパケットの最小の受信信号強度インジケータ（RSSI）値を指定するには、**config advanced 802.11 coverage rssi-threshold** コマンドを使用します。

config advanced 802.11{**a** | **b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
data	データ パケットのしきい値を指定します。
voice	音声パケットのしきい値を指定します。
rssi	有効な値は –60 ～ –90 dBm です。

コマンド デフォルト

- データ パケットのデフォルトの RSSI 値は -80 dBm です。
- 音声パケットのデフォルトの RSSI 値は -75 dBm です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

入力した *rssi* 値は、ネットワーク内のカバレッジ ホール（カバレッジが不完全な領域）を特定するために使用されます。入力した値よりも小さい RSSI 値を持つパケットが、アクセス ポイントのデータ キューまたは音声キューで受信されると、カバレッジ ホールの可能性が検出されます。

アクセス ポイントでは、5 秒ごとに RSSI が測定され、90 秒間隔でそれらがコントローラに報告されます。

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジ ホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global** コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、802.11a アクセス ポイントが受信したデータ パケットに対して最小の受信信号強度インジケータを設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a coverage rssi-threshold -60
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage

config advanced 802.11 edca-parameters

802.11a ネットワーク上で、特定の拡張型分散チャネル アクセス（EDCA）プロファイルを有効にするには、**config advanced 802.11 edca-parameters** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **edca-parameters** {**wmm-default** | **svp-voice** | **optimized-voice** | **optimized-video-voice** | **custom-voice** | | **custom-set** { *QoS Profile Name* } { **aifs** *AP-value (0-16) Client value (0-16)* | **ecwmax** *AP-Value (0-10) Client value (0-10)* | **ecwmin** *AP-Value (0-10) Client value (0-10)* | **txop** *AP-Value (0-255) Client value (0-255)* } }

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
wmm-default	Wi-Fi Multimedia（WMM）デフォルト パラメータを有効にします。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
svp-voice	Spectralink 音声優先パラメータを有効にします。通話の質を向上するため、ネットワークに Spectralink 電話技術を実装している場合に、このオプションを選択します。
optimized-voice	EDCA 音声最適化パラメータを有効にします。Spectralink 以外の音声サービスをネットワーク上で展開している場合に、このオプションを選択します。
optimized-video-voice	音声およびビデオ用に最適化された EDCA プロファイル パラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。 （注） ビデオ サービスを展開する場合は、アドミッション制御を無効にする必要があります。
custom-voice	802.11a のカスタム音声 EDCA パラメータをイネーブルにします。このオプションの EDCA パラメータは、このプロファイルが適用された場合、6.0 WMM EDCA パラメータとも一致します。

custom-set	EDCA パラメータのカスタマイズを有効にします。 • **aifs—Configures the Arbitration Inter-Frame Space.** **AP Value (0-16) Client value (0-16)** • **ecwmax—Configures the maximum Contention Window.** **AP Value(0-10) Client Value (0-10)** • **ecwmin—Configures the minimum Contention Window.** **AP Value(0-10) Client Value(0-10)** • **txop—Configures the Arbitration Transmission Opportunity Limit.** **AP Value(0-255) Client Value(0-255)** QoS プロファイル名：QoS プロファイル名を入力します。 • bronze • silver • Gold • platinum

コマンド デフォルト

デフォルトの EDCA パラメータは **wmm-default** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.2.110.0	このリリースで、edca-parameters コマンドに custom-set キーワードが追加されました。

例

次に、Spectralink 音声優先パラメータを有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 edca-parameters svp-voice
```

関連コマンド

config advanced 802.11b edca-parameters	802.11aネットワーク上で、特定の拡張型分散チャネル アクセス（EDCA）プロファイルを有効にします。
show 802.11a	802.11aネットワークの基本的な設定を表示します。

config advanced 802.11 factory

802.11a の詳細設定を工場出荷時のデフォルトにリセットするには、**config advanced 802.11 factory** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **factory**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての 802.11a の詳細設定を工場出荷時のデフォルトに戻す例を示します。

```
(Cisco Controller) > config advanced 802.11a factory
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11 group-member

802.11 静的 RF グループのメンバを設定するには、**config advanced 802.11 group-member** コマンドを使用します。

config advanced 802.11{**a** | **b**} **group-member**{**add** | **remove**} *controller controller-ip-address*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
add	静的 RF グループにコントローラを追加します。
remove	静的RF グループからコントローラを除外します。
controller	追加するコントローラの名前。
controller-ip-address	追加するコントローラの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a 自動 RF グループにコントローラを追加する例を示します。

```
(Cisco Controller) > config advanced 802.11a group-member add cisco-controller
209.165.200.225
```

関連コマンド

show advanced 802.11a group

config advanced 802.11 group-mode

config advanced 802.11 group-mode

802.11aの自動RFグループ選択モードをオンまたはオフに設定するには、**config advanced 802.11 group-mode** コマンドを使用します。

config advanced 802.11{**a** | **b**} **group-mode** {**auto** | **leader** | **off** | **restart**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
auto	802.11a RF グループ選択を自動更新モードに設定します。
leader	802.11a RF グループ選択をスタティック モードに設定し、グループ リーダーとしてこのコントローラを設定します。
off	802.11aRF グループ選択をオフに設定します。
restart	802.11a RF グループ選択を再起動します。

コマンド デフォルト

802.11a の自動 RF グループ選択モードは、デフォルトでは auto になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a の自動 RF グループ選択モードをオンに設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a group-mode auto
```

次に、802.11a の自動 RF グループ選択モードをオフに設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a group-mode off
```

関連コマンド

show advanced 802.11a group

config advanced 802.11 group-member

config advanced 802.11 logging channel

チャネル変更ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging channel** コマンドを使用します。

config advanced 802.11{**a** | **b**} **logging channel** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
logging channel	チャネル変更をロギングします。
on	802.11 チャネルのロギングを有効にします。
off	802.11 チャネルのロギングを無効にします。

コマンド デフォルト

デフォルトのチャネル変更ロギング モードはオフ（無効）です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a ロギング チャネル選択モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging channel on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging channel

config advanced 802.11 logging coverage

カバレッジ プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging coverage** コマンドを使用します。

config advanced 802.11{**a** | **b**} **logging coverage** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 のカバレッジ プロファイル違反ロギングを有効にします。
off	802.11 のカバレッジ プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトのカバレッジ プロファイル ロギング モードはオフ（無効）です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a カバレッジ プロファイル違反ロギング選択モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging coverage on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging coverage

config advanced 802.11 logging foreign

外部干渉プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging foreign** コマンドを使用します。

config advanced 802.11{**a** | **b**} **logging foreign** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 外部干渉プロファイル違反ロギングを有効にします。
off	802.11 外部干渉プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトの外部干渉プロファイル ロギング モードはオフ（無効）です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a外部干渉プロファイル違反ロギング選択モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging foreign on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging foreign

config advanced 802.11 logging load

802.11a 負荷プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging load** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **logging load** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 負荷プロファイル違反ロギングを有効にします。
off	802.11 負荷プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトの 802.11 a 負荷プロファイル ロギング モードはオフ (無効) です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a 負荷プロファイル ロギング モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11 logging load on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging load

config advanced 802.11 logging noise

802.11a ノイズ プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging noise** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **logging noise** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 ノイズ プロファイル違反ロギングを有効にします。
off	802.11 ノイズ プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトの 802.11 a ノイズ プロファイル ロギング モードはオフ (無効) です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ノイズ プロファイル ロギング モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging noise on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging noise

config advanced 802.11 logging performance

802.11aパフォーマンス プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging performance** コマンドを使用します。

config advanced 802.11{**a** | **b**} **logging performance** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 パフォーマンス プロファイル違反ロギングを有効にします。
off	802.11 パフォーマンス プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトの 802.11 a パフォーマンス プロファイル ロギング モードはオフ (無効) です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a パフォーマンス プロファイル ロギング モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging performance on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging performance

config advanced 802.11 logging txpower

802.11a 伝送パワー変更ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging txpower** コマンドを使用します。

config advanced 802.11{**a** | **b**} **logging txpower** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 伝送パワー変更のロギングを有効にします。
off	802.11 伝送パワー変更のロギングを無効にします。

コマンド デフォルト

デフォルトの 802.11 a 伝送パワー変更ロギング モードはオフ（無効）です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a 伝送パワー変更モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11 logging txpower off
```

関連コマンド

show advanced 802.11 logging

config advanced 802.11b logging power

config advanced 802.11 monitor channel-list

802.11a ノイズ、干渉、および不正な監視チャネル リストを設定するには、**config advanced 802.11 monitor channel-list** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **monitor channel-list** {**all** | **country** | **dca**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
all	すべてのチャネルを監視します。
country	設定されている国コードで使用するチャネルを監視します。
dca	自動チャネル割り当てで使用するチャネルを監視します。

コマンド デフォルト

802.11a ノイズ、干渉、および不正な監視チャネル リストは、デフォルトでは country に設定されています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、設定されている国で使用するチャネルを監視する例を示します。

```
(Cisco Controller) > config advanced 802.11 monitor channel-list country
```

関連コマンド

show advanced 802.11a monitor coverage

config advanced 802.11 monitor load

負荷測定間隔を 60 ～ 3,600 秒に設定するには、**config advanced 802.11 monitor load** コマンドを使用します。

config advanced 802.11{**a** | **b**} **monitor load** *seconds*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
seconds	60 ～ 3,600 秒の負荷測定間隔。

コマンド デフォルト

デフォルトの負荷測定間隔は 60 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、負荷測定間隔を 60 秒に設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 monitor load 60
```

関連コマンド

show advanced 802.11a monitor

config advanced 802.11b monitor load

config advanced 802.11 monitor measurement

信号測定間隔を 60 ～ 3,600 秒に設定するには、**config advanced 802.11 monitor measurement** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **monitor measurement** *seconds*

構文の説明

seconds	入力する必要がある信号測定間隔。有効な範囲は、60 ～ 3600 秒です。

コマンド デフォルト

デフォルトの信号測定間隔は 180 秒です。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、信号測定間隔を 300 秒に設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 monitor measurement 300
```

config advanced 802.11 monitor mode

802.11aアクセス ポイントの監視を有効または無効にするには、**config advanced 802.11 monitor mode** コマンドを使用します。

config advanced 802.11{**a** | **b**} **monitor mode** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	802.11 アクセス ポイントの監視を有効にします。
disable	802.11 アクセス ポイントの監視を無効にします。

コマンド デフォルト

802.11 a アクセス ポイントの監視は、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a アクセス ポイントの監視を有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11a monitor mode enable
```

関連コマンド

show advanced 802.11a monitor

config advanced 802.11b monitor mode

config advanced 802.11 monitor ndp-type

802.11 アクセス ポイントの無線リソース管理（RRM）ネイバー ディスカバリ プロトコル（NDP）タイプを設定するには、**config advanced 802.11 monitor ndp-type** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **monitor ndp-type** {**protected** | **transparent**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
protected	Tx RRM によって保護された NDP を指定します。
transparent	Tx RRM の透過的な NDP を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

802.11 アクセス ポイントの RRM NDP タイプを設定する前に、**config 802.11 disable network** コマンドを入力して、ネットワークを無効にしたことを確認します。

次に、802.11a アクセス ポイント RRM NDP タイプを protected として有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 monitor ndp-type protected
```

関連コマンド

config advanced 802.11 monitor

config advanced 802.11 monitor mode

config advanced 802.11 disable

config advanced 802.11 monitor timeout-factor

802.11 ネイバー タイムアウト要因を設定するには、**config advanced 802.11 monitor timeout-factor** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **monitor timeout-factor** *factor-value-in-minutes*

構文の説明

factor-value-in-minutes	入力する必要のあるネイバー タイムアウト要因の値。有効な範囲は 5 ～ 60 分です。タイムアウト要因を 60 分に設定することをお勧めします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

config advanced 802.11 optimized roaming

各 802.11 帯域の最適化されたローミングのパラメータを設定するには、**config advanced 802.11 optimized roaming** コマンドを使用します。

config advanced {**802.11a** | **802.11b**} **optimized-roaming** {**enable** | **disable** | **interval** *seconds* | **datarate** *mbps*}

構文の説明

802.11a	802.11a ネットワークの最適化されたローミングのパラメータを設定します。
802.11b	802.11b ネットワークの最適化されたローミングのパラメータを設定します。
enable	最適化されたローミングを有効にします。
disable	最適化されたローミングを無効にします。
interval	802.11a/b ネットワークのクライアント カバレッジのレポート間隔を設定します。
seconds	クライアント カバレッジのレポート間隔（秒単位）。範囲は 5 ～ 90 秒です。
datarate	802.11a/b ネットワークのしきい値データ レートを設定します。
mbps	802.11a/b ネットワークのしきい値データ レート（Mbps 単位）。 802.11a の場合、設定可能なデータ レートは 6、9、12、18、24、36、48、および 54 です。 802.11b の場合、設定可能なデータ レートは、1、2、5.5、11、6、9、12、18、24、36、48、および 54 です。 データ レートを 無効にしてクライアントの関連付けを解除するには 0 を設定します。

コマンド デフォルト

デフォルトでは、ローミングの最適化は無効になっています。クライアント カバレッジのレポート間隔のデフォルト値は 90 秒、しきい値データ レートのデフォルト値は 0（無効状態）です。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

ローミングの最適化のレポート間隔を設定する前に、802.11a/b ネットワークを無効にする必要があります。レポートの間隔に対して低い値を設定すると、カバレッジ レポートのメッセージでネットワークが過負荷になることがあります。

次に、802.11a ネットワークの最適化されたローミングを有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11a optimized roaming enable
```

次に、802.11 a ネットワークのデータ レート間隔を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a optimized roaming datarate 9
```

config advanced 802.11 packet

最大パケット再試行回数、連続パケット障害しきい値、およびデフォルトタイムアウト値を設定するには、**config advanced 802.11 packet** コマンドを使用します。

config advanced 802.11 {**a** | **b**} < *QoS Profile Name* > { **max-client-count** <*threshold value (0-1000)*> | **max-packet-count** <*threshold value (0-1000)*> | **max-retry** <*maximum retry count*> | **timeout** <*time(in miliseconds)*> }

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
QoS Profile Name	• bronze • silver • Gold • platinum
max-client-count	クライアントの関連付けを解除するまでの連続パケット障害しきい値を設定します。 *threshold value*：クライアント数しきい値を 0 ー 1000 の範囲で入力します。
max-packet-count	障害パケットの再試行をやめるまでの連続パケット障害しきい値を設定します。 *threshold value*：パケット障害しきい値を 0 ー 1000 の範囲で入力します。
max-retry	障害パケットのパケット再試行回数を設定します。 *maximum retry count*：再試行の最大許容回数を入力します。
timeout	パケット エージングまたは廃棄タイムアウトしきい値を設定します。 *time*：パケットがタイムアウトするまでの最大時間を入力します。

コマンド デフォルト

config advanced 802.11 packet コマンドのパラメータのデフォルト値は次のとおりです。

キーワード	デフォルト値
max-client-count	500

キーワード	デフォルト値
max-packet-count	100
max-retry	3
timeout	35 ミリ秒

コマンド履歴

リリース	変更内容
8.2	このリリースで packet コマンドが追加されました。

```
(Cisco Controller) > config advanced 802.11a packet platinum max-packet-count 200
```

関連コマンド

show 802.11a	802.11a ネットワークの基本的な設定を表示します。

config advanced 802.11 profile clients

Cisco Lightweight アクセス ポイントのクライアント数のしきい値を 1 ～ 75 に設定するには、**config advanced 802.11 profile clients** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **profile clients** {**global** | *cisco_ap*} *clients*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての 802.11a 対応 Cisco Lightweight アクセス ポイントを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
clients	802.11a 対応 Cisco Lightweight アクセス ポイントのクライアント数のしきい値（1 ～ 75）。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのクライアント数のしきい値は、デフォルトでは 12 に設定されています。

次に、すべての Cisco Lightweight アクセス ポイントのクライアント数のしきい値を 25 に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile clients global 25
Global client count profile set.
```

次に、AP1 のクライアント数のしきい値を 75 に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile clients AP1 75
Global client count profile set.
```

config advanced 802.11 profile customize

802.11a 対応 Cisco Lightweight アクセス ポイントのパフォーマンス プロファイルのカスタマイズをオンまたはオフにするには、**config advanced 802.11 profile customize** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **profile customize** *cisco_ap* {**on** | **off**}

構文の説明

a	802.11a/n ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント。
on	この Cisco Lightweight アクセス ポイントのパフォーマンス プロファイルをカスタマイズします。
off	この Cisco Lightweight アクセス ポイントに対してグローバルデフォルト パフォーマンス プロファイルを使用します。

コマンド デフォルト

パフォーマンス プロファイルのカスタマイズは、デフォルトではオフになっています。

次に、802.11a 対応 Cisco Lightweight アクセス ポイント AP1 のパフォーマンス プロファイルのカスタマイズをオンにする例を示します。

```
(Cisco Controller) >config advanced 802.11 profile customize AP1 on
```

config advanced 802.11 profile foreign

外部 802.11a トランスミッタ干渉しきい値を 0 ～ 100 % に設定するには、**config advanced 802.11 profile foreign** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **profile foreign** {**global** | *cisco_ap*} *percent*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての 802.11a 対応 Cisco Lightweight アクセス ポイントを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
percent	0 ～ 100 % の外部 802.11a 干渉しきい値。

コマンド デフォルト

デフォルトの外部 802.11a トランスミッタ干渉しきい値は 10 です。

次に、すべての Cisco Lightweight アクセス ポイントの外部 802.11a トランスミッタ干渉しきい値を 50 % に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11a profile foreign global 50
```

次に、AP1 の外部 802.11a トランスミッタ干渉しきい値を 0 % に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile foreign AP1 0
```

config advanced 802.11 profile noise

802.11a 外部ノイズしきい値を -127 ～ 0 dBm に設定するには、**config advanced 802.11 profile noise** コマンドを使用します。

config advanced 802.11{**a** | **b**} **profile noise** {**global** | *cisco_ap*} *dBm*

構文の説明

a	802.11a/n ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
global	すべての 802.11a 対応 Cisco Lightweight アクセス ポイントの特定のプロファイルを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
dBm	-127 ～ 0 dBm の 802.11a 外部ノイズしきい値。

コマンド デフォルト

デフォルトの外部ノイズしきい値は –70 dBm です。

次に、すべての Cisco Lightweight アクセス ポイントの 802.11a 外部ノイズしきい値を –127 dBm に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11a profile noise global -127
```

次に、AP1 の 802.11a 外部ノイズしきい値を 0 dBm に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11a profile noise AP1 0
```

config advanced 802.11 profile throughput

Cisco Lightweight アクセス ポイントのデータレート スループットしきい値を 1,000 ～ 10,000,000 バイト/秒に設定するには、**config advanced 802.11 profile throughput** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **profile throughput** {**global** | *cisco_ap*} *value*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての 802.11a 対応 Cisco Lightweight アクセス ポイントの特定のプロファイルを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
value	802.11a 対応 Cisco Lightweight アクセス ポイントのスループットしきい値（1,000 ～ 10,000,000 バイト/秒）。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのデフォルトのデータレート スループットしきい値は 1,000,000 バイト/秒です。

次に、すべての Cisco Lightweight アクセス ポイントのデータ レートしきい値を 1,000 バイト/秒に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile throughput global 1000
```

次に、AP1 のデータ レートしきい値を 10,000,000 バイト/秒に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile throughput AP1 10000000
```

config advanced 802.11 profile utilization

RF 利用率のしきい値を 0 ～ 100 % に設定するには、**config advanced 802.11 profile utilization** コマンドを使用します。オペレーティング システムがこのしきい値を超えた場合にトラップを生成します。

config advanced 802.11 {**a** | **b**} **profile utilization** {**global** | *cisco_ap*} *percent*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	グローバルの Cisco Lightweight アクセス ポイント固有のプロファイルを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
percent	0 ～ 100 % の 802.11a の RF 利用率のしきい値。

コマンド デフォルト

RF 利用率のデフォルトのしきい値は 80% です。

次に、すべての Cisco Lightweight アクセス ポイントの RF 利用率のしきい値を 0 % に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile utilization global 0
```

次に、AP1 の RF 利用率のしきい値を 100 % に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile utilization AP1 100
```

config advanced 802.11 receiver

詳細なレシーバ設定を行うには、**config advanced 802.11 receiver** コマンドを使用します。

config advanced 802.11{**a** | **b**} **receiver** {**default** | **rxstart jumpThreshold** *value*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
receiver	レシーバ設定を指定します。
default	デフォルトの詳細なレシーバ設定を指定します。
rxstart jumpThreshold	レシーバ起動信号を指定します。 （注） このオプションは、シスコ社内専用であるため、使用しないことをお勧めします。
value	ジャンプしきい値設定の値（0 ～ 127）。

コマンド デフォルト

なし

使用上のガイドライン

- 802.11 レシーバ設定を変更する前に、802.11 ネットワークを無効にする必要があります。
- **rxstart jumpThreshold** *value* オプションは、シスコ社内専用であるため、使用しないことをお勧めします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ネットワークが有効なとき次にレシーバパラメータを変更できないようにする例を示します。

```
(Cisco Controller) > config advanced 802.11 receiver default
```

config advanced 802.11 reporting measurement

レポート測定間隔を 60 ～ 3,600 秒に設定するには、**config advanced 802.11 reporting measurement** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **reporting measurement** *seconds*

構文の説明

seconds	入力する必要があるレポート測定間隔。有効な範囲は、60 ～ 3600 秒です。

コマンド デフォルト

デフォルトのレポート測定間隔は 180 秒です。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、信号測定間隔を 300 秒に設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 reporting measurement 300
```

config advanced 802.11 tpc-version

無線の送信電力の制御（TPC）バージョンを設定するには、**config advanced 802.11 tpc-version** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpc-version** {**1** | **2**}

構文の説明

1	強力な信号カバレッジおよび安定性を提供する TPC バージョン 1 を指定します。
2	音声コールが広く使用されるシナリオ用の TPC バージョン 2 を指定します。干渉を最小にするために、送信電力が動的に調整されます。これは、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジ ホールのインシデントが多く発生する可能性があります。

コマンド デフォルト

無線のデフォルトの TPC のバージョンは 1 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a 無線の 1 として TPC のバージョンを設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a tpc-version 1
```

関連コマンド

config advanced 802.11 tpcv1-thresh

config advanced 802.11 tpcv1-thresh

無線の送信電力の制御（TPC）バージョン1のしきい値を設定するには、**config advanced 802.11 tpcv1-thresh** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpcv1-thresh** *threshold*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
threshold	50 dBm ～ 80 dBm の範囲のしきい値。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a 無線の TPC バージョン 1 でしきい値を -60 dBm として設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 tpcv1-thresh -60
```

関連コマンド

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-intense

無線の送信電力の制御（TPC）バージョン 2 の算出の強度を設定するには、**config advanced 802.11 tpcv2-intense** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpcv2-intense** *intensity*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
intensity	1～100 の算出の強度。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a 無線の TPC バージョン 2 で算出の強度を 50 として設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 tpcv2-intense 50
```

関連コマンド

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-per-chan

config advanced 802.11 tpcv2-per-chan

送信電力の制御バージョン 2 をチャネル単位で設定するには、**config advanced 802.11 tpcv2-per-chan** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpcv2-per-chan** {**enable** | **disable**}

構文の説明

enable	TPC バージョン 2 の設定をチャネル単位で有効にします。
disable	TPC バージョン 2 の設定をチャネル単位で無効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a 無線の TPC バージョン 2 をチャネル単位で有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 tpcv2-per-chan enable
```

関連コマンド

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-intense

config advanced 802.11 tpcv2-thresh

無線の送信電力の制御（TPC）バージョン2のしきい値を設定するには、**config advanced 802.11 tpcv2-thresh** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpcv2-thresh** *threshold*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
threshold	50 dBm ～ 80 dBm の範囲のしきい値。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a 無線の TPC バージョン 2 でしきい値を -60 dBm として設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a tpcv2-thresh -60
```

関連コマンド

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv1-thresh

config advanced 802.11 tpcv2-per-chan

config advanced 802.11 txpower-update

すべての Cisco Lightweight アクセス ポイントで 802.11a 伝送パワーの更新を開始するには、**config advanced 802.11 txpower-update** コマンドを使用します。

config advanced 802.11{**a** | **b**} **txpower-update**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a アクセス ポイントで 802.11a 伝送パワーの更新を開始する例を示します。

```
(Cisco Controller) > config advanced 802.11 txpower-update
```

関連コマンド

config advance 802.11b txpower-update

config advanced eap

詳細な拡張認証プロトコル（EAP）設定を行うには、**config advanced eap** コマンドを使用します。

config advanced eap {**bcast-key-interval** *seconds* | **eapol-key-timeout** *timeout* | **eapol-key-retries** *retries* | **identity-request-timeout** *timeout* | **identity-request-retries** *retries* | **key-index** *index* | **max-login-ignore-identity-response** {**enable** | **disable**} **request-timeout** *timeout* | **request-retries** *retries*}

構文の説明

bcast-key-interval *seconds*	EAP ブロードキャスト キー更新間隔を秒単位で指定します。 範囲は 120 ～ 86400 秒です。
eapol-key-timeout *timeout*	EAP または WPA/WPA-2 PSK を使用してコントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信するまでに待機する時間（200 ～ 5000 ミリ秒）を指定します。 デフォルト値は 1000 ミリ秒です。
eapol-key-retries *retries*	コントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信する最大回数（0～4）を指定します。 デフォルト値は 2 です。
identity-request- timeout *timeout*	コントローラが無線クライアントに EAP ID 要求メッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
identity-request- retries	コントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信する最大回数（0～4）を指定します。 デフォルト値は 2 です。
key-index *index*	ダイナミック Wired Equivalent Privacy（WEP）で使用するキーインデックス（0 または 3）を指定します。

max-login-ignore- identity-response	有効になっている場合、このコマンドは、802.1x 認証を使用して同じユーザ名のコントローラに接続可能なデバイスの数に対して設定されている制限を無視します。ディセーブルにすると、このコマンドは、コントローラに同じユーザ名で接続できるデバイスの数を制限します。このオプションは、Web認証ユーザには適用されません。 同じユーザ名で接続できるデバイスの最大数を制限するには、**config netuser maxUserLogin** コマンドを使用します。
enable	最大EAP ID応答に到達する同じユーザ名を無視します。
disable	最大EAP ID応答に到達する同じユーザ名を確認します。
request-timeout	ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
request-retries	（任意）ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信する最大回数（0 ～ 20）を指定します。 デフォルト値は 2 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ダイナミック Wired Equivalent Privacy（WEP）に使用するキー インデックスを設定する例を示します。

```
(Cisco Controller) > config advanced eap key-index 0
```

関連コマンド **show advanced eap**

config advanced hotspot

高度なホットスポット設定を指定するには、**config advanced hotspot** コマンドを使用します。

config advanced hotspot {**anqp-4way** {**disable** | **enable** | **threshold** *value* } | **cmbk-delay** *value* | **garp** {**disable** | **enable** } | **gas-limit** {**disable** | **enable** }}

構文の説明

anqp-4way	Network Query Protocol（ANQP）4-way フラグメントのしきい値をイネーブル化、ディセーブル化、または設定します。
disable	ANQP 4-way メッセージをディセーブルにします。
enable	ANQP 4-way メッセージをイネーブルにします。
threshold	ANQP 4-way フラグメントのしきい値を設定します。
value	バイト単位の ANQP 4-way フラグメントのしきい値。範囲は 10 ～ 1500 です。デフォルト値は 1500 です
cmbk-delay	時間単位（TU）の ANQP の戻り遅延を設定します。
value	時間単位（TU）の ANQP の戻り遅延。1 TU は、1024 usec として 802.11 で定義されています。指定できる範囲は 1～ 30 秒です。
garp	ワイヤレス ネットワークへの Gratuitous ARP（GARP）転送をディセーブルまたはイネーブルにします。
disable	ワイヤレス ネットワークへの Gratuitous ARP（GARP）転送をディセーブルにします。
enable	ワイヤレス ネットワークへの Gratuitous ARP（GARP）転送をイネーブルにします。
gas-limit	指定した間隔で、アクセス ポイントによりスイッチに送信される Generic Advertisement Service（GAS）要求アクション フレームの数を制限します。
disable	アクセス ポイントの GAS 要求アクション フレームの制限をディセーブルにします。
enable	アクセス ポイントの GAS 要求アクション フレームの制限をイネーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に ANQP 4-way フラグメントのしきい値を設定する例を示します。

```
(Cisco Controller) >config advanced hotspot anqp-4way threshold 200
```

config advanced timers auth-timeout

認証タイムアウトを設定するには、**config advanced timers auth-timeout** コマンドを使用します。

config advanced timers auth-timeout *seconds*

構文の説明

seconds	10 ～600 秒の認証応答タイムアウト値。

コマンド デフォルト

デフォルトの認証タイムアウト値は 10 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、認証タイムアウトを 20 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced timers eap-timeout

拡張可能認証プロトコル（EAP）有効期限タイムアウトを設定するには、**config advanced timers eap-timeout** コマンドを使用します。

config advanced timers eap-timeout *seconds*

構文の説明

seconds	8 ～ 120 秒の EAP タイムアウト値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、EAP 有効期限タイムアウトを 10 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers eap-timeout 10
```

config advanced timers eap-identity-request-delay

詳細な拡張可能認証プロトコル（EAP）アイデンティティ要求遅延を秒単位で設定するには、**config advanced timers eap-identity-request-delay** コマンドを使用します。

config advanced timers eap-identity-request-delay *seconds*

構文の説明

seconds	0 ～ 10 秒の詳細な EAP ID 要求遅延。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、詳細な EAP アイデンティティ要求遅延を 8 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers eap-identity-request-delay 8
```

config advanced timers

高度なシステム タイマーを設定するには、**config advanced timers** コマンドを使用します。

config advanced timers {**ap-coverage-report** *seconds* | **ap-discovery-timeout** *discovery-timeout* | **ap-fast-heartbeat** {**local** | **flexconnect** | **all**} {**enable** | **disable**} *fast_heartbeat_seconds* | **ap-heartbeat-timeout** *heartbeat_seconds* | **ap-primary-discovery-timeout** *primary_discovery_timeout* | **ap-primed-join-timeout** *primed_join_timeout* | **auth-timeout** *auth_timeout* | **pkt-fwd-watchdog** {**enable** | **disable**} {*watchdog_timer* | **default**} | **eap-identity-request-delay** *eap_identity_request_delay* | **eap-timeout** *eap_timeout*}

構文の説明

ap-coverage-report	すべての AP の RRM カバレッジ レポート間隔を設定します。
seconds	AP のカバレッジ レポート間隔を秒単位で設定します。範囲は 60 ~ 90 秒です。デフォルトは 90 秒です。
ap-discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウト値を設定します。
discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウト値（秒単位）。値の範囲は 1 ～ 10 です。
ap-fast-heartbeat	アクセス ポイントのコントローラ障害を検出するために要する時間を短縮する高速ハートビート タイマーを設定にします。
local	ローカル モードのアクセス ポイントの高速ハートビート間隔を設定します。
flexconnect	FlexConnect モードのアクセス ポイントの高速ハートビート間隔を設定します。
all	すべてのアクセス ポイントの高速ハートビート間隔を設定します。
enable	ファーストハートビート間隔を有効にします。
disable	ファーストハートビート間隔を無効にします。
fast_heartbeat_seconds	コントローラ障害を検出するために要する時間を短縮する小さい値のハートビート間隔（秒単位）。値の範囲は 1 ～ 10 です。
ap-heartbeat-timeout	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値を設定します。

heartbeat_seconds	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値（秒単位）。値の範囲は 1 ～ 30 です。この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。
ap-primary-discovery-timeout	アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。
primary_discovery_timeout	アクセス ポイントのプライマリ検出要求時間（秒単位）。範囲は 30 ～ 3600 です。
ap-primed-join-timeout	アクセス ポイントのプライミングされた検出タイムアウト値を設定します。
primed_join_timeout	アクセス ポイントのプライミングされた検出タイムアウト値（秒単位）。範囲は 120 ～ 43200 です。
auth-timeout	認証タイムアウトを設定します。
auth_timeout	認証応答タイムアウト値（秒単位）。範囲は 10 ～ 600 です。
pkt-fwd-watchdog	ファストパスのデッドロックから保護するためのパケット転送ウォッチドッグ タイマーを設定します。
watchdog_timer	パケット転送ウォッチドッグ タイマー（秒単位）。範囲は 60 ～ 300 です。
default	ウォッチドッグ タイマーをデフォルト値の 240 秒に設定します。
eap-identity-request-delay	詳細な拡張可能認証プロトコル（EAP）アイデンティティ要求遅延を秒単位で設定します。
eap_identity_request_delay	詳細な EAP アイデンティティ要求遅延（秒単位）。範囲は 0 ～ 10 です。
eap-timeout	EAP 有効期限タイムアウトを設定します。
eap_timeout	EAP タイムアウト値（秒単位）。範囲は 8 ～ 120 です。

コマンド デフォルト

- デフォルトのアクセス ポイント検出タイムアウトは 10 秒です。
- デフォルトのアクセス ポイント ハートビート タイムアウトは 30 秒です。

- デフォルトのアクセス ポイント プライマリ検出要求タイマーは 120 秒です。
- デフォルトの認証タイムアウトは 10 秒です。
- デフォルトのパケット転送ウォッチドッグ タイマーは 240 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.3	コマンドの機能が拡張されました。

使用上のガイドライン

Cisco Lightweight アクセス ポイントの検出タイムアウトとは、Cisco WLC が、接続されていない Cisco Lightweight アクセス ポイントの検出を試行する頻度です。

Cisco Lightweight アクセス ポイントのハートビート タイムアウトは、Cisco Lightweight アクセス ポイントが Cisco Wireless LAN Controller にハートビート キープアライブ信号を送信する頻度を制御します。

次に、タイムアウト値を 20 でアクセス ポイント検出タイムアウトを設定する例を示します。

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

次に、FlexConnect モードのアクセス ポイントを対象に高速ハートビート間隔を有効にする例を示します。

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```

次に、認証タイムアウトを 20 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced fastpath fastcache

ファストパスのファスト キャッシュ制御を設定するには、**config advanced fastpath fastcache** コマンドを使用します。

config advanced fastpath fastcache {**enable** | **disable**}

構文の説明

enable	ファストパスのファスト キャッシュ制御をイネーブルにします。
disable	ファストパスのファストキャッシュ制御をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ファストパスのファスト キャッシュ制御を有効にする例を示します。

```
(Cisco Controller) > config advanced fastpath fastcache enable
```

関連コマンド

config advanced fastpath pkt-capture

config advanced fastpath pkt-capture

ファストパスのパケット キャプチャを設定するには、**config advanced fastpath pkt-capture** コマンドを使用します。

config advanced fastpath pkt-capture {**enable** | **disable**}

構文の説明

enable	ファストパスのパケット キャプチャをイネーブルにします。
disable	ファストパスのパケットキャプチャをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ファストパスのパケット キャプチャを有効にする例を示します。

```
(Cisco Controller) > config advanced fastpath pkt-capture enable
```

関連コマンド

config advanced fastpath fastcache

config advanced sip-preferred-call-no

音声優先制御を設定するには、**config advanced sip-preferred-call-no** コマンドを使用します。

config advanced sip-preferred-call-no *call_index* {*call_number* | **none**}

構文の説明

call_index	1 ～ 6 の間の有効な値を持つコール インデックス。
call_number	27 文字まで使用できる優先コール数。
none	指定されたインデックスにセットされている優先コールを削除します。

コマンド デフォルト

なし

使用上のガイドライン

音声優先制御を設定する前に、次の前提条件を実行する必要があります。

- **config wlan qos** *wlan-id* **platinum** コマンドを入力して、音声をプラチナ QoS レベルに設定します。
- **config 802.11** {**a** | **b**} **cac** {**voice** | **video**} **acm enable** コマンドを入力して、この無線に対するアドミッション コントロール（ACM）を有効にします。
- **config wlan call-snoop enable** *wlan-id* コマンドを入力して、特定の WLAN に対するコールスヌーピング機能を有効にします。

  優先コールの統計情報を表示するには、**show ap stats** {**802.11**{**a** | **b**} | **wlan**} *cisco_ap* コマンドを入力します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、インデックス 2 に、新しい優先コールを追加する例を示します。

```
(Cisco Controller) > config advanced sip-preferred-call-no 2 0123456789
```

関連コマンド

config wlan qos

config 802.11 cac video acm

config 802.11 cac voice acm

config wlan call-snoop

show ap stats

config advanced sip-snooping-ports

コール スヌーピング ポートを設定するには、**config advanced sip-snooping-ports** コマンドを使用します。

config advanced sip-snooping-ports *start_port end_port*

構文の説明

start_port	コール スヌーピング用の開始ポート。範囲は 0 ～ 65535 です。
end_port	コール スヌーピング用の終了ポート。範囲は 0 ～ 65535 です。

使用上のガイドライン

コール スヌーピング用に 1 つのポートしか必要ない場合は、開始ポートと終了ポートを同じ番号に設定します。

CIUS タブレットで使用されるポートは 5060 で、Facetime で使用されるポート範囲は 16384 ～ 16402 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コール スヌーピング ポートを設定する例を示します。

```
(Cisco Controller) > config advanced sip-snooping-ports 4000 4500
```

関連コマンド

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video sip

config 802.11 cac voice sip

show advanced sip-preferred-call-no

show advanced sip-snooping-ports

debug cac

config advanced backup-controller primary

プライマリ バックアップ コントローラを設定するには、**config advanced backup-controller primary** コマンドを使用します。

config advanced backup-controller primary *system name IP addr*

構文の説明

system name	プライマリ	セカンダリ バックアップ コントローラを設定します。
ip-addr	バックアップ コントローラの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

プライマリ バックアップ コントローラ エントリ（IPv6 または IPv4）を削除するには、コントローラの IP アドレスとして 0.0.0.0 と入力します。

次に、IPv4 プライマリ バックアップ コントローラを設定する例を示します。

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 10.10.10.10
```

次に、IPv6 プライマリ バックアップ コントローラを設定する例を示します。

```
(Cisco Controller) >config advanced backup-controller primary systemname 2001:9:6:40::623
```

次に、IPv4 プライマリ バックアップ コントローラを削除する例を示します。

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 10.10.10.10
```

次に、IPv6 プライマリ バックアップ コントローラを削除する例を示します。

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 0.0.0.0
```

関連コマンド

show advanced back-up controller

config advanced backup-controller secondary

セカンダリ バックアップ コントローラを設定するには、**config advanced backup-controller secondary** コマンドを使用します。

config advanced backup-controller secondary *system name IP addr*

構文の説明

system name	プライマリ	セカンダリ バックアップ コントローラを設定します。
ip-addr	バックアップ コントローラの IP アドレス。

コマンド デフォルト

なし

使用上のガイドライン

セカンダリ バックアップ コントローラ エントリ（IPv4 または IPv6）を削除するには、コントローラの IP アドレスとして 0.0.0.0 と入力します。

次に、IPv4 セカンダリ バックアップ コントローラを設定する例を示します。

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 10.10.10.10
```

次に、IPv6 セカンダリ バックアップ コントローラを設定する例を示します。

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2
2001:9:6:40::623
```

次に、IPv4 セカンダリ バックアップ コントローラを削除する例を示します。

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

次に、IPv6 セカンダリ バックアップ コントローラを削除する例を示します。

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

関連コマンド

show advanced back-up controller

config advanced client-handoff

802.11 データ パケットの再試行が指定した回数に達した時点でクライアント ハンドオフが行われるように設定するには、**config advanced client-handoff** コマンドを使用します。

config advanced client-handoff *num_of_retries*

構文の説明

num_of_retries	クライアント ハンドオフが行われる前の再試行数の限度（0 ～ 255）。

コマンド デフォルト

802.11 データ パケットの再試行数の限度のデフォルト値は 0 です。

次に、クライアント ハンドオフを再試行数の限度 100 に設定する例を示します。

```
(Cisco Controller) >config advanced client-handoff 100
```

config advanced dot11-padding

Over-the-Air フレーム パディングを有効または無効にするには、**config advanced dot11-padding** コマンドを使用します。

config advanced dot11-padding {**enable** | **disable**}

構文の説明

enable	Over-the-Air フレーム パディングを有効にします。
disable	Over-the-Air フレーム パディングを無効にします。

コマンド デフォルト

Over-the-Air フレーム パディングは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Over-the-Air フレーム パディングを有効にする例を示します。

```
(Cisco Controller) > config advanced dot11-padding enable
```

関連コマンド

debug dot11

debug dot11 mgmt interface

debug dot11 mgmt msg

debug dot11 mgmt ssid

debug dot11 mgmt state-machine

debug dot11 mgmt station

show advanced dot11-padding

config advanced assoc-limit

アクセス ポイント無線がアソシエーション要求および認証要求をコントローラに送信するレートを設定するには、**config advanced assoc-limit** コマンドを使用します。

config advanced assoc-limit {**enable** [*number of associations per interval* | *interval*] | **disable**}

構文の説明

enable	アクセス ポイントごとのアソシエーション要求の設定を有効にします。
disable	アクセス ポイントごとのアソシエーション要求の設定を無効にします。
number of associations per interval	（任意）指定した間隔での 1 つのアクセス ポイント スロットあたりのアソシエーション要求数。範囲は 1 ～ 100 です。
interval	（任意）アソシエーション要求制限間隔。範囲は 100 ～ 10000 ミリ秒です。

コマンド デフォルト

このコマンドのデフォルト状態は無効です。

使用上のガイドライン

200 以上の無線クライアントが同時にコントローラにアソシエートしようとする際、**config advanced assoc-limit** コマンドを使用してアクセス ポイントからのアソシエーション要求を制限している場合は、クライアントが DHCP_REQD のステータスにとどまることはなくなります。

次に、20 の指定した間隔での 1 つのアクセス ポイント スロットあたりのアソシエーション要求数を 250 のアソシエーション要求制限間隔で設定する例を示します。

```
(Cisco Controller) >config advanced assoc-limit enable 20 250
```

config advanced max-1x-sessions

各アクセス ポイントに許可されている同時802.1Xセッションの最大数を設定するには、**config advanced max-1x-sessions** コマンドを使用します。

config advanced max-1x-sessions *no_of_sessions*

構文の説明

no_of_sessions	一度の AP あたりの 802.1x セッション開始の最大数。範囲は 0～255 で、0 は無制限を示します。

コマンド デフォルト

なし

次に、同時 802.1X セッションの最大数を設定する例を示します。

```
(Cisco Controller) >config advanced max-1x-sessions 200
```

config advanced rate

スイッチ制御パス レート制限を設定するには、**config advanced rate** コマンドを使用します。

config advanced rate {**enable** | **disable**}

構文の説明

enable	スイッチ制御パス レート制限機能を有効にします。
disable	スイッチ制御パス レート制限機能を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、スイッチ制御パス レート制限を有効にする例を示します。

```
(Cisco Controller) >config advanced rate enable
```

config advanced probe backoff

Cisco AP のプローブ キューのバックオフ パラメータを設定するには、**config advanced probe backoff** コマンドを使用します。

config advanced probe backoff {**enable** | **disable**}

構文の説明

enable	プローブ応答にデフォルトのバックオフ パラメータ値を使用する場合に選択します。
disable	プローブ応答に増加されたバックオフ パラメータを使用する場合に選択します。

コマンド デフォルト

無効

次に、プローブ応答に増加されたバックオフ パラメータを使用する例を示します。

```
(Cisco Controller) >config advanced probe backoff enable
```

config advanced probe filter

アクセス ポイントからコントローラに転送されたプローブ要求のフィルタリングを設定するには、**config advanced probe filter** コマンドを入力します。

config advanced probe filter {**enable** | **disable**}

構文の説明

enable	プローブ要求のフィルタリングを有効にします。
disable	プローブ要求のフィルタリングを無効にします。

コマンド デフォルト

なし

次に、アクセス ポイントからコントローラに転送されたプローブ要求のフィルタリングを有効にする例を示します。

```
(Cisco Controller) >config advanced probe filter enable
```

config advanced probe limit

指定された間隔での、1 つのクライアントおよび 1 つのアクセス ポイントあたりの WLAN コントローラに送信されるプローブ数を制限するには、**config advanced probe limit** コマンドを入力します。

config advanced probe limit *num_probesinterval*

構文の説明

num_probes	指定された間隔での、1 つのアクセス ポイント無線および 1 つのクライアントあたりのプローブ要求数（1 ～ 100）。
interval	プローブ制限間隔（100 ～ 10,000 ミリ秒）。

コマンド デフォルト

プローブ要求のデフォルト数は 2 です。デフォルトの間隔は 500 ミリ秒です。

次に、1つのクライアントおよび1つのアクセスポイントあたりのプローブ数を5に、プローブ間隔を 800 ミリ秒に設定する例を示します。

```
(Cisco Controller) >config advanced probe limit 5 800
```

config advanced timers

高度なシステム タイマーを設定するには、**config advanced timers** コマンドを使用します。

config advanced timers {**ap-coverage-report** *seconds* | **ap-discovery-timeout** *discovery-timeout* | **ap-fast-heartbeat** {**local** | **flexconnect** | **all**} {**enable** | **disable**} *fast_heartbeat_seconds* | **ap-heartbeat-timeout** *heartbeat_seconds* | **ap-primary-discovery-timeout** *primary_discovery_timeout* | **ap-primed-join-timeout** *primed_join_timeout* | **auth-timeout** *auth_timeout* | **pkt-fwd-watchdog** {**enable** | **disable**} {*watchdog_timer* | **default**} | **eap-identity-request-delay** *eap_identity_request_delay* | **eap-timeout** *eap_timeout*}

構文の説明

ap-coverage-report	すべての AP の RRM カバレッジ レポート間隔を設定します。
seconds	AP のカバレッジ レポート間隔を秒単位で設定します。範囲は 60 ~ 90 秒です。デフォルトは 90 秒です。
ap-discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウト値を設定します。
discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウト値（秒単位）。値の範囲は 1 ～ 10 です。
ap-fast-heartbeat	アクセス ポイントのコントローラ障害を検出するために要する時間を短縮する高速ハートビート タイマーを設定にします。
local	ローカル モードのアクセス ポイントの高速ハートビート間隔を設定します。
flexconnect	FlexConnect モードのアクセス ポイントの高速ハートビート間隔を設定します。
all	すべてのアクセス ポイントの高速ハートビート間隔を設定します。
enable	ファーストハートビート間隔を有効にします。
disable	ファーストハートビート間隔を無効にします。
fast_heartbeat_seconds	コントローラ障害を検出するために要する時間を短縮する小さい値のハートビート間隔（秒単位）。値の範囲は 1 ～ 10 です。
ap-heartbeat-timeout	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値を設定します。

heartbeat_seconds	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値（秒単位）。値の範囲は 1 ～ 30 です。この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。
ap-primary-discovery-timeout	アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。
primary_discovery_timeout	アクセス ポイントのプライマリ検出要求時間（秒単位）。範囲は 30 ～ 3600 です。
ap-primed-join-timeout	アクセス ポイントのプライミングされた検出タイムアウト値を設定します。
primed_join_timeout	アクセス ポイントのプライミングされた検出タイムアウト値（秒単位）。範囲は 120 ～ 43200 です。
auth-timeout	認証タイムアウトを設定します。
auth_timeout	認証応答タイムアウト値（秒単位）。範囲は 10 ～ 600 です。
pkt-fwd-watchdog	ファストパスのデッドロックから保護するためのパケット転送ウォッチドッグ タイマーを設定します。
watchdog_timer	パケット転送ウォッチドッグ タイマー（秒単位）。範囲は 60 ～ 300 です。
default	ウォッチドッグ タイマーをデフォルト値の 240 秒に設定します。
eap-identity-request-delay	詳細な拡張可能認証プロトコル（EAP）アイデンティティ要求遅延を秒単位で設定します。
eap_identity_request_delay	詳細な EAP アイデンティティ要求遅延（秒単位）。範囲は 0 ～ 10 です。
eap-timeout	EAP 有効期限タイムアウトを設定します。
eap_timeout	EAP タイムアウト値（秒単位）。範囲は 8 ～ 120 です。

コマンド デフォルト

- デフォルトのアクセス ポイント検出タイムアウトは 10 秒です。
- デフォルトのアクセス ポイント ハートビート タイムアウトは 30 秒です。

- デフォルトのアクセス ポイント プライマリ検出要求タイマーは 120 秒です。
- デフォルトの認証タイムアウトは 10 秒です。
- デフォルトのパケット転送ウォッチドッグ タイマーは 240 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。
8.3	コマンドの機能が拡張されました。

使用上のガイドライン

Cisco Lightweight アクセス ポイントの検出タイムアウトとは、Cisco WLC が、接続されていない Cisco Lightweight アクセス ポイントの検出を試行する頻度です。

Cisco Lightweight アクセス ポイントのハートビート タイムアウトは、Cisco Lightweight アクセス ポイントが Cisco Wireless LAN Controller にハートビート キープアライブ信号を送信する頻度を制御します。

次に、タイムアウト値を 20 でアクセス ポイント検出タイムアウトを設定する例を示します。

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

次に、FlexConnectモードのアクセス ポイントを対象に高速ハートビート間隔を有効にする例を示します。

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```

次に、認証タイムアウトを 20 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config ap 802.1Xuser

コントローラに現在関連付けられているアクセス ポイント、および今後関連付けられるすべてのアクセス ポイントについて、グローバル認証のユーザ名とパスワードを設定するには、**config ap 802.1Xuser** コマンドを使用します。

config ap 802.1Xuser add username *ap-username* **password** *ap-password* {**all** | *cisco_ap*}

構文の説明

add username	ユーザ名を追加することを指定します。
ap-username	Cisco AP でのユーザ名。
password	パスワードを追加することを指定します。
ap-password	パスワード。
cisco_ap	特定のアクセス ポイント。
all	すべてのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

強度が高いパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

特定のアクセス ポイントの値を設定できます。

次に、すべてのアクセス ポイントにグローバル認証ユーザ名およびパスワードを設定する例を示します。

```
(Cisco Controller) >config ap 802.1Xuser add username cisco123 password cisco2020 all
```

config ap 802.1Xuser delete

特定のアクセス ポイントがコントローラのグローバル認証設定を使用するように強制するには、**config ap 802.1Xuser delete** コマンドを使用します。

config ap 802.1Xuser delete *cisco_ap*

構文の説明

cisco_ap	アクセス ポイント。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、コントローラのグローバル認証設定を使用するアクセス ポイント AP01 を削除する例を示します。

```
(Cisco Controller) >config ap 802.1Xuser delete AP01
```

config ap 802.1Xuser disable

すべてのアクセス ポイントまたは特定のアクセス ポイントの認証を無効にするには、**config ap 802.1Xuser disable** コマンドを使用します。

config ap 802.1Xuser disable {**all** | *cisco_ap* }

構文の説明

disable	認証を無効にします。
all	すべてのアクセス ポイントを指定します。
cisco_ap	アクセス ポイント。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

特定のアクセス ポイントの 802.1X 認証は、グローバル 802.1X 認証が有効でない場合にだけ無効にできます。グローバル 802.1X 認証が有効な場合は、すべてのアクセス ポイントに対してだけ 802.1X を無効にできます。

次に、アクセス ポイント cisco_ap1 の認証を無効にする例を示します。

```
(Cisco Controller) >config ap 802.1Xuser disable
```

config advanced dot11-padding

Over-the-Air フレーム パディングを有効または無効にするには、**config advanced dot11-padding** コマンドを使用します。

config advanced dot11-padding {**enable** | **disable**}

構文の説明

enable	Over-the-Air フレーム パディングを有効にします。
disable	Over-the-Air フレーム パディングを無効にします。

コマンド デフォルト

Over-the-Air フレーム パディングは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Over-the-Air フレーム パディングを有効にする例を示します。

```
(Cisco Controller) > config advanced dot11-padding enable
```

関連コマンド

debug dot11

debug dot11 mgmt interface

debug dot11 mgmt msg

debug dot11 mgmt ssid

debug dot11 mgmt state-machine

debug dot11 mgmt station

show advanced dot11-padding

config ap

Cisco Lightweight アクセス ポイントを設定する、またはサードパーティ（外部）アクセス ポイントを追加または削除するには、**config ap** コマンドを使用します。

config ap {{**enable** | **disable**} *cisco_ap* | {**add** | **delete**} *MAC port* {**enable** | **disable**} *IP_address*}

構文の説明

enable	Cisco Lightweight アクセス ポイントを有効にします。
disable	Cisco Lightweight アクセス ポイントを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
add	外部アクセス ポイントを追加します。
delete	外部アクセス ポイントを削除します。
MAC	外部アクセス ポイントの MAC アドレス。
port	外部アクセス ポイントに到達できるポート番号。
IP_address	外部アクセス ポイントの IP アドレス。

コマンド デフォルト

なし

次に、Lightweight アクセス ポイント AP1 を無効にする例を示します。

```
(Cisco Controller) >config ap disable AP1
```

次に、MAC アドレスが 12:12:12:12:12:12、IP アドレスが 192.12.12.1 の外部アクセス ポイントをポート 2033 から追加する例を示します。

```
(Cisco Controller) >config ap add 12:12:12:12:12:12 2033 enable 192.12.12.1
```

config ap aid-audit

Cisco Lightweight アクセス ポイントの AID 監査メカニズムを設定するには、**config ap aid-audit** コマンドを使用します。

config ap aid-audit {**enable** | **disable**}

構文の説明

aid-audit	AID 監査メカニズムを設定します。
enable	AID 監査メカニズムを有効にします。
disable	AID 監査メカニズムを無効にします。

コマンド デフォルト

ディセーブル

コマンド履歴

リリース	変更内容
8.6	このコマンドが導入されました。

次に、AP で AID 監査を有効にする例を示します。

```
(Cisco Controller) >config ap aid-audit enable
```

config ap antenna band-mode

Cisco AP のアンテナのバンドモードをシングルまたはデュアルとして設定するには、**config ap antenna band-mode** コマンドを使用します。

config ap antenna band-mode {**single** | **dual**} *cisco-ap*

構文の説明

single	Cisco AP のシングル バンド アンテナ モードを設定します。
dual	Cisco AP のデュアル バンド アンテナ モードを設定します。
cisco-ap	Cisco AP の名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。
8.3 以降のリリース	**antenna-band-mode** パラメータが **antenna band-mode** に変更されました。

config ap atf 802.11

config ap atf 802.11 コマンドを使用することにより、AP レベルで Cisco Air Time Fairness を設定します。

config ap atf 802.11{**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} *ap-name*} | {**optimization** {**enable** | **disable**}}

構文の説明

a	802.11a ネットワーク設定を指定します。
b	802.11b/g ネットワーク設定を指定します。
mode	Cisco ATF の強制のきめ細かさを設定します。
disable	Cisco ATF を無効にします。
monitor	Cisco ATF をモニタ モードで設定します。
enforce-policy	Cisco ATF を強制モードで設定します。
ap-name	指定する必要がある AP 名。
optimization	通信時間の最適化を設定します。
enable	通信時間の最適化を有効にします。
disable	通信時間の最適化を無効にします。

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

802.11a ネットワークで Cisco AP（*my-ap*）の通信時間の最適化を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config ap atf 802.11a optimization enable my-ap
```

config ap atf 802.11 policy

WLAN で Cisco ATF ポリシーの AP レベルのオーバーライドを設定するには、次のコマンドを入力します。

confit ap atf 802.11{**a** | **b**} **policy** *wlan-id policy-name ap-name* **override** {**enable** | **disable**}

構文の説明

a	802.11a ネットワーク設定を指定します。
b	802.11b ネットワーク設定を指定します。
policy	Cisco ATF ポリシーを指定します。
wlan-id	指定する必要がある WLAN ID またはリモート LAN ID。
policy-name	指定する必要がある Cisco ATF ポリシー名。
ap-name	指定する必要がある AP 名。
override	AP グループの WLAN の ATF ポリシー オーバーライドを設定します。
enable	AP グループの WLAN の ATF ポリシー オーバーライドを有効にします。
disable	AP グループの WLAN の ATF ポリシー オーバーライドを無効にします。

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

config ap autoconvert

Cisco WLC と関連付けるときに、すべてのアクセス ポイントを FlexConnect モードまたは Monitor モードに自動的に変換するには、**config ap autoconvert** コマンドを使用します。

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

構文の説明

flexconnect	FlexConnect モードへのすべてのアクセス ポイントが自動的に設定されます。
monitor	モニタ モードへのすべてのアクセス ポイントが自動的に設定されます。
disable	アクセス ポイントに対する autoconvert オプションをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ローカル モードのアクセス ポイントが Cisco 7500 シリーズ ワイヤレス コントローラに接続している場合、そのアクセス ポイントはクライアントにサービスを提供しません。アクセス ポイントの詳細はコントローラで使用できます。アクセス ポイントが Cisco 7500 シリーズ ワイヤレス コントローラに接続しているときに、クライアントにサービスを提供できる、またはモニタ関連のタスクを実行できるようにするには、アクセス ポイントのモードを FlexConnect モードまたは Monitor モードにします。

このコマンドは、Cisco 5520、8540、および 8510 シリーズ ワイヤレス コントローラ プラットフォームでの AP モードの変換にも使用できます。

次に、すべてのアクセス ポイントを FlexConnect モードに自動的に変換する例を示します。

```
(Cisco Controller) >config ap autoconvert flexconnect
```

次に、AP の自動変換オプションを無効にする例を示します。

```
(Cisco Controller) >config ap autoconvert disable
```

config ap bhrate

Cisco Bridge Backhaul Tx Rate を設定するには、**config ap bhrate** コマンドを使用します。

config ap bhrate {*rate* | **auto**} *cisco_ap*

構文の説明

rate	Cisco Bridge Backhaul Tx Rate（Kbps）。有効な値は、6000、12000、18000、24000、36000、48000、および 54000 です。
auto	自動データ レートを設定します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

コマンドのデフォルトのステータスは auto に設定されています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

以前のソフトウェア リリースでは、ブリッジデータ レートのデフォルト値は24000（24 Mbps）でした。コントローラ ソフトウェアのリリース 6.0 では、ブリッジ データ レートのデフォルト値は **auto** です。以前のコントローラ ソフトウェアのリリースでデフォルトのブリッジ データ レート値（24000）を設定した場合は、コントローラ ソフトウェア リリース 6.0 にアップグレードしたときにブリッジデータ レートが新しいデフォルト値（auto）で設定されます。ただし、以前のコントローラ ソフトウェアのリリースでデフォルト値以外の値（たとえば、18000）を設定した場合は、Cisco WLC リリース 6.0 にアップグレードしたときにその設定が保持されます。

ブリッジデータ レートが **auto** に設定されている場合、メッシュ バックホールは最大レートを選択します。次に大きいレートは、（すべてのレートではなく）その特定のレートが不適切な状況にあるため、使用できません。

次に、Cisco Bridge Backhaul Tx Rate を 54000 kbps に設定する例を示します。

```
(Cisco Controller) >config ap bhrate 54000 AP01
```

config ap bridgegroupname

Cisco Lightweight アクセス ポイントでブリッジ グループ名を設定または削除するには、**config ap bridgegroupname** コマンドを使用します。

config ap bridgegroupname {**set** *groupname* | **delete** | {**strict-matching** {**enable** | **disable**}}}*cisco_ap*

構文の説明

set	Cisco Lightweight アクセス ポイントのブリッジ グループ名を設定します。
groupname	ブリッジ グループ名
delete	Cisco Lightweight アクセス ポイントのブリッジ グループ名を削除します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
strict-matching	MAP にデフォルト以外のブリッジ グループ名が設定されており、潜在的な親に異なるブリッジ グループ名が設定されている場合、可能な親のリストを制限します。
enable	Cisco Lightweight アクセス ポイントのグループ名を有効にします。
disable	Cisco Lightweight アクセス ポイントのグループ名を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	**strict-matching** パラメータが追加されました。

使用上のガイドライン

同じブリッジ グループ名を持つアクセス ポイントだけが相互に接続できます。AP ブリッジ グループ名を変更すると、ブリッジ AP が残る場合があります。

次に、Cisco アクセス ポイントのブリッジ グループ名 AP02 でブリッジ グループ名を削除する例を示します。

```
(Cisco Controller) >config ap bridgegroupname delete AP02
Changing the AP's bridgegroupname may strand the bridge AP. Please continue with caution.
Changing the AP's bridgegroupname will also cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

config ap bridging

Cisco Lightweight アクセス ポイントでのイーサネット間ブリッジングを設定するには、**config ap bridging** コマンドを使用します。

config ap bridging {**enable** | **disable**} *cisco_ap*

構文の説明

enable	Cisco Lightweight アクセス ポイントでのイーサネット間ブリッジングを有効にします。
disable	イーサネット間ブリッジングを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントでブリッジングを有効にする例を示します。

```
(Cisco Controller) >config ap bridging enable nyc04-44-1240
```

次に、アクセス ポイントでブリッジングを無効にする例を示します。

```
(Cisco Controller) >config ap bridging disable nyc04-44-1240
```

config ap cdp

Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を設定するには、**config ap cdp** コマンドを使用します。

config ap cdp {**enable** | **disable** | **interface** {**ethernet** *interface_number* | **slot** *slot_id*}} {*cisco_ap* | **all**}

構文の説明

enable	アクセス ポイントで CDP を有効にします。
disable	アクセス ポイントで CDP を無効にします。
interface	特定のインターフェイスの CDP を設定します。
ethernet	イーサネットインターフェイスの CDP を設定します。
interface_number	0～3 のイーサネットインターフェイス番号。
slot	無線インターフェイスの CDP を設定します。
slot_id	0～3 のスロット番号。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントを指定します。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

コマンド デフォルト

メッシュ AP の無線インターフェイスで有効になっていて、非メッシュ AP の無線インターフェイスで無効になっています。すべての AP のイーサネット インターフェイスで有効になっています。

使用上のガイドライン

config ap cdp disable all コマンドは、コントローラに join しているすべてのアクセス ポイントおよび今後 join するすべてのアクセス ポイントの CDP を無効にします。CDP は、コントローラまたはアクセス ポイントのリブート後も現在と将来のアクセス ポイントで無効のままになります。CDP を有効にするには、**config ap cdp enable all** コマンドを入力します。

（注） イーサネット/無線インターフェイス上の CDP は、CDP が有効になっている場合にだけ使用できます。コントローラに join しているすべてのアクセス ポイントで CDP を有効にした後、**config ap cdp** {**enable** | **disable**} *cisco_ap* コマンドを使用して個々のアクセス ポイントで CDP を無効にした後再び有効にできます。コントローラに join されたすべてのアクセス ポイントで CDP を無効にした後は、個々のアクセス ポイントで CDP を有効にし、無効にすることはできません。

次に、すべてのアクセス ポイントで CDP を有効にする例を示します。

```
(Cisco Controller) >config ap cdp enable all
```

次に ap02 アクセス ポイントで CDP を無効にする例を示します。

```
(Cisco Controller) >config ap cdp disable ap02
```

次に、すべてのアクセス ポイントでイーサネット インターフェイス番号 2 の CDP を有効にする例を示します。

```
(Cisco Controller) >config ap cdp ethernet 2 enable all
```

config ap core-dump

Cisco Lightweight アクセス ポイントのメモリ コア ダンプを設定するには、**config ap core-dump** コマンドを使用します。

config ap core-dump {**disable** | **enable** *tftp_server_ipaddress filename* {**compress** | **uncompress**} {*cisco_ap* | **all**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのメモリ コア ダンプ設定を有効にします。
disable	Cisco Lightweight アクセス ポイントのメモリ コア ダンプ設定を無効にします。
tftp_server_ipaddress	アクセス ポイントがコア ダンプ ファイルを送信する Trivial File Transfer Protocol（TFTP）サーバの IP アドレス。
filename	コア ファイルのラベルを付けるためにアクセス ポイントが使用する名前。
compress	コア ダンプ ファイルを圧縮します。
uncompress	コア ダンプ ファイルを圧縮解除します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントを指定します。

（注） AP 自体が「all」という名前で設定されている場合、「all access points」の場合は「all」という名前の AP に優先します。

コマンド デフォルト

なし

使用上のガイドライン

アクセス ポイントは TFTP サーバに到達できる必要があります。このコマンドは、IPv4 と IPv6 の両方のアドレスに適用されます。

次に、コア ダンプ ファイルを設定して圧縮する例を示します。

```
(Cisco Controller) >config ap core-dump enable 209.165.200.225 log compress AP02
```

config ap crash-file clear-all

すべてのクラッシュおよび無線コア ダンプ ファイルを削除するには、**config ap crash-file clear-all** コマンドを使用します。

config ap crash-file clear-all

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、すべてのクラッシュ ファイルを削除する例を示します。

```
(Cisco Controller) >config ap crash-file clear-all
```

config ap crash-file delete

単一のクラッシュまたは無線コア ダンプ ファイルを削除するには、**config ap crash-file delete** コマンドを使用します。

config ap crash-file delete *filename*

構文の説明

filename	削除するファイルの名前を指定します。

コマンド デフォルト

なし

次に、クラッシュ ファイル 1 を削除する例を示します。

```
(Cisco Controller) >config ap crash-file delete crash_file_1
```

config ap crash-file get-crash-file

Cisco Lightweight アクセス ポイントの最新のクラッシュ データを収集するには、**config ap crash-file get-crash-file** コマンドを使用します。

config ap crash-file get-crash-file *cisco_ap*

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

使用上のガイドライン

transfer upload datatype コマンドを使用して、Cisco Wireless LAN Controller に収集されたデータを転送します。

次に、アクセス ポイント A3 の最新のクラッシュ データを収集する例を示します。

```
(Cisco Controller) >config ap crash-file get-crash-file AP3
```

config ap crash-file get-radio-core-dump

Cisco Lightweight アクセス ポイントの無線コア ダンプを取得するには、**config ap crash-file get-radio-core-dump** コマンドを使用します。

config ap crash-file get-radio-core-dump *slot_id cisco_ap*

構文の説明

slot_id	スロット ID（0 または 1）。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

次に、アクセス ポイント AP02 とスロット 0 の無線コア ダンプを収集する例を示します。

```
(Cisco Controller) >config ap crash-file get-radio-core-dump 0 AP02
```

config ap dtls-cipher-suite

AP とコントローラの間の DTLS 接続用の新しい暗号スイートを有効にするには、**config ap dtls-cipher-suite** コマンドを使用します。

config ap dtls-cipher-suite {**RSA-AES256-SHA256** | **RSA-AES256-SHA** | **RSA-AES128-SHA**}

構文の説明

RSA-AES256-SHA256	RSA キー交換または認証を使用する暗号スイート（256 ビット AES と SHA 256 を使用）。
RSA-AES256-SHA	RSA キー交換または認証を使用する暗号スイート（256 ビット AES と SHA を使用）。
RSA-AES128-SHA	RSA キー交換または認証を使用する暗号スイート（128 ビット AES と SHA を使用）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、AP とコントローラの間の DTLS 接続に 256 ビット AES と SHA 256 を使用する RSA 暗号スイートを有効にする例を示します。

```
(Cisco Controller) > config ap dtls-cipher-suite RSA-AES256-SHA256
```

config ap ethernet duplex

Lightweight アクセス ポイントのイーサネット ポート デュプレックスおよび速度を設定するには、**config ap ethernet duplex** コマンドを使用します。

config ap ethernet duplex［**auto** | **half** | **full**］ **speed**［**auto** | **10** | **100** | **1000**］｛ **all** | *cisco_ap* ｝

構文の説明

auto	（任意）イーサネット ポートの自動二重設定を指定します。
half	（任意）イーサネット ポートの半二重設定を指定します。
full	（任意）イーサネット ポートの全二重設定を指定します。
speed	イーサネットポート速度の設定を指定します。
auto	（任意）イーサネット ポート速度を自動に指定します。
10	（任意）イーサネット ポート速度を 10 Mbps に指定します。
100	（任意）イーサネット ポート速度を 100 Mbps に指定します。
1000	（任意）イーサネット ポート速度を 1000 Mbps に指定します。
all	接続されているすべてのアクセス ポイントにイーサネット ポートの設定を指定します。
cisco_ap	シスコ アクセス ポイント。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのアクセス ポイントで 10 Mbps としてイーサネット ポートの半二重を設定する例を示します。

```
(Cisco Controller) >config ap ethernet duplex half speed 10 all
```

config ap ethernet tag

Control and Provisioning of Wireless Access Points（CAPWAP）パケットの VLAN タギングを設定するには、**config ap ethernet tag** コマンドを使用します。

config ap ethernet tag {**id** *vlan_id* | **disable**} {*cisco_ap* | **all**}

構文の説明

id	VLAN ID を指定します。
vlan_id	トランク VLAN の ID。
disable	VLAN タグ機能を無効にします。VLAN タグ機能を無効にすると、アクセス ポイントは CAPWAP パケットのタグ付けを解除します。
cisco_ap	Cisco AP の名前。
all	すべての Cisco アクセス ポイントに VLAN タギングを設定します。

コマンド デフォルト

なし

使用上のガイドライン

VLAN タギングを設定すると、その設定はアクセス ポイントがリブートした後で有効になります。

メッシュ アクセス ポイントには VLAN タギングを設定できません。

アクセス ポイントが指定したトランク VLAN を使用してトラフィックをルーティングできないか、コントローラに到達できない場合は、タグなし設定にフォールバックします。アクセス ポイントがこのフォール バック設定を使用してコントローラに接続すると、コントローラは Cisco Prime Infrastructure などのトラップ サーバにトランク VLAN の障害を示すトラップを送信します。このシナリオでは、show コマンドの出力に「Failover to untagged」というメッセージが表示されます。

次に、トランク VLAN に VLAN タギングを設定する例を示します。

```
(Cisco Controller) >config ap ethernet tag 6 AP1
```

config ap autoconvert

Cisco WLC と関連付けるときに、すべてのアクセス ポイントを FlexConnect モードまたは Monitor モードに自動的に変換するには、**config ap autoconvert** コマンドを使用します。

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

構文の説明

flexconnect	FlexConnect モードへのすべてのアクセス ポイントが自動的に設定されます。
monitor	モニタ モードへのすべてのアクセス ポイントが自動的に設定されます。
disable	アクセス ポイントに対する autoconvert オプションをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ローカル モードのアクセス ポイントが Cisco 7500 シリーズ ワイヤレス コントローラに接続している場合、そのアクセス ポイントはクライアントにサービスを提供しません。アクセス ポイントの詳細はコントローラで使用できます。アクセス ポイントが Cisco 7500 シリーズ ワイヤレス コントローラに接続しているときに、クライアントにサービスを提供できる、またはモニタ関連のタスクを実行できるようにするには、アクセス ポイントのモードを FlexConnect モードまたは Monitor モードにします。

このコマンドは、Cisco 5520、8540、および 8510 シリーズ ワイヤレス コントローラ プラットフォームでの AP モードの変換にも使用できます。

次に、すべてのアクセス ポイントを FlexConnect モードに自動的に変換する例を示します。

```
(Cisco Controller) >config ap autoconvert flexconnect
```

次に、AP の自動変換オプションを無効にする例を示します。

```
(Cisco Controller) >config ap autoconvert disable
```

config ap flexconnect bridge

Flex+ブリッジアクセス ポイントでFlexConnectブリッジバックホールを設定するには、**config ap flexconnect bridge** コマンドを使用します。

config ap flexconnect bridge {**backhaul-wlan** | **resilient**} *cisco_ap* {**enable** | **disable**}

構文の説明

backhaul-wlan	FlexConnect AP でバックホール WLAN を有効にします。
resilient	Flex+ブリッジ AP でスタンドアロン モードを有効にします。
cisco_ap	アクセス ポイントの名前。
enable	アクセス ポイントで選択されたモードを有効にします。
disable	アクセス ポイントで選択されたモードを無効にします。

コマンド デフォルト

Flex + ブリッジ AP でデフォルトの高復元力モードが有効になっています。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、AP で高復元力モードを有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect bridge resilient AP2 enable
```

config ap flexconnect central-dhcp

WLAN の FlexConnect アクセス ポイントで中央 DHCP を有効にするには、**config ap flexconnect central-dhcp** コマンドを使用します。

config ap flexconnect central-dhcp *wlan_id cisco_ap* [**add** | **delete**] {**enable** | **disable**} **override dns** {**enable** | **disable**} **nat-pat** {**enable** | **disable**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
add	（任意）新しい WLAN DHCP マッピングを追加します。
delete	（任意）WLAN DHCP マッピングを削除します。
enable	FlexConnect アクセス ポイントで中央 DHCP を有効にします。この機能を有効にすると、アクセス ポイントから受信した DHCP パケットは、コントローラに中央でスイッチされ、次に AP と SSID に基づいて対応する VLAN に転送されます。
disable	FlexConnect アクセス ポイントで中央 DHCP を無効にします。
override dns	コントローラによって割り当てられたインターフェイス上の DNS サーバ アドレスを上書きします。中央でスイッチされる WLAN で DNS を上書きすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
enable	FlexConnect アクセス ポイントのオーバーライド DNS 機能を有効にします。
disable	FlexConnect アクセス ポイントのオーバーライド DNS 機能を無効にします。
nat-pat	有効または無効に設定できるネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）。
enable	FlexConnect アクセス ポイントで NAT-PAT を有効にします。
disable	FlexConnect アクセス ポイントで NAT-PAT を削除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、中央 DHCP、オーバーライド DNS、および FlexConnect アクセス ポイントの NAT-PAT を有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect central-dhcp 1 ap1250 enable override dns
enable nat-pat enable
```

config ap flexconnect local-split

FlexConnect アクセス ポイントのローカル スプリット トンネルを設定するには、 **config ap flexconnect local-split** コマンドを使用します。

config ap flexconnect local-split *wlan_id cisco_ap* {**enable** | **disable**} **acl** *acl_name*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	FlexConnect アクセス ポイントの名前。
enable	FlexConnect アクセス ポイントでローカル スプリット トンネルを有効にします。
disable	FlexConnect アクセス ポイントでローカル スプリット トンネルを無効にします。
acl	FlexConnect のローカル スプリット アクセス コントロール リストを設定します。
acl_name	FlexConnect のアクセス コントロール リストの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用すると、FlexConnect ACL を使用して、中央でスイッチされる WLAN にローカル スプリット トンネルを設定することができます。NAT/PAT はマルチキャスト IP トラフィックをサポートしないため、ローカル スプリット トンネルがサポートするのはユニキャスト レイヤ 4 IP トラフィックのみです。

次に、FlexConnect ACL を使用してローカル スプリット トンネルを設定する例を示します。

```
(Cisco Controller) >config ap flexconnect local-split 6 AP2 enable acl flex6
```

config ap flexconnect module-vlan

FlexConnect ローカル スイッチングにおける Cisco USC 8x18 デュアル モード モジュール用の VLAN タギングを設定するには、**config ap flexconnect module-vlan** コマンドを使用します。

config ap flexconnect module-vlan {{**enable** *ap-name* [**vlan** *vlan-id*]} | {{**disable** | **remove**} *ap-name*}}

構文の説明

enable *ap-name*	指定された Cisco AP の外部モジュールに対し、ネイティブ VLAN を使用して FlexConnect ローカル スイッチングを有効にします。
enable *ap-name* **vlan** *vlan-id*	指定された Cisco AP の外部モジュールに対し、非ネイティブ VLAN を使用して FlexConnect ローカル スイッチングを有効にします。
disable *ap-name*	指定された Cisco AP の外部モジュールに対して FlexConnect ローカル スイッチングを無効にします。
remove *ap-name*	AP 固有の外部モジュール VLAN 設定を削除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、Cisco AP の外部モジュールに対し、非ネイティブ VLAN を使用して FlexConnect ローカル スイッチングを有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect module-vlan enable 3600i-ap vlan4
```

config ap flexconnect policy

FlexConnect アクセス ポイントのポリシー ACL を設定するには、**config ap flexconnect policy** コマンドを使用します。

config ap flexconnect policy {**add** | **delete**} *acl_name*

構文の説明

add	FlexConnect アクセス ポイントのポリシー ACL を追加します。
deletes	FlexConnect アクセス ポイントのポリシー ACL を削除します。
acl_name	ACL の名前

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

次に、FlexConnect アクセス ポイントのポリシー ACL を追加する例を示します。

```
(Cisco Controller) >config ap flexconnect policy add acl1
```

config ap flexconnect radius auth set

特定の FlexConnect アクセス ポイントのプライマリまたはセカンダリ RADIUS サーバを設定するには、**config ap flexconnect radius auth set** コマンドを使用します。

config ap flexconnect radius auth set {**primary** | **secondary**} *ip_address auth_port secret*

構文の説明

primary	特定の FlexConnect アクセス ポイントのプライマリ RADIUS サーバを指定します。
secondary	特定の FlexConnect アクセス ポイントのセカンダリ RADIUS サーバを指定します。
ip_address	RADIUS サーバの IP アドレス。
auth_port secret	ポート名
secret	RADIUS サーバのシークレット

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、特定のアクセス ポイントのプライマリ RADIUS サーバを設定する例を示します。

```
(Cisco Controller) >config ap flexconnect radius auth set primary 192.12.12.1
```

config ap flexconnect vlan

FlexConnect アクセスの VLAN タギングを有効または無効にするには、**config ap flexconnect vlan** コマンドを使用します。

config ap flexconnect vlan {**enable** | **disable**} *cisco_ap*

構文の説明

enable	アクセス ポイントの VLAN タギングを有効にします。
disable	アクセス ポイントの VLAN タギングを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

ディセーブルローカル スイッチに対していったん有効化された WLAN は、Cisco WLC で割り当てられた VLAN を継承します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect アクセスのアクセス ポイントの VLAN タギングを有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect vlan enable AP02
```

config ap flexconnect vlan add

FlexConnect アクセス ポイントに VLAN を追加するには、**config ap flexconnect vlan add** コマンドを使用します。

config ap flexconnect vlan add *vlan-id acl in-acl out-acl cisco_ap*

構文の説明

vlan-id	VLAN 識別番号。
acl	最大 32 文字の英数字による ACL 名。
in-acl	最大 32 文字の英数字による着信 ACL 名。
out-acl	最大 32 文字の英数字による発信 ACL 名。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect アクセス ポイントを設定する例を示します。

```
(Cisco Controller) >config ap flexconnect vlan add 21 acl inacl1 outacl1 ap1
```

config ap flexconnect vlan native

FlexConnect アクセス ポイントのネイティブ VLAN を設定するには、**config ap flexconnect vlan native** コマンドを使用します。

config ap flexconnect vlan native *vlan-id cisco_ap*

構文の説明

vlan-id	VLAN 識別番号。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect アクセス ポイント モードにネイティブ VLAN を設定する例を示します。

```
(Cisco Controller) >config ap flexconnect vlan native 6 AP02
```

config ap flexconnect vlan wlan

FlexConnect アクセス ポイントに VLAN ID を割り当てるには、**config ap flexconnect vlan wlan** コマンドを使用します。

config ap flexconnect vlan wlan *wlan-id vlan-id cisco_ap*

構文の説明

wlan-id	WLAN 識別子。
vlan-id	VLAN 識別子（1 ~ 4094）。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

WLAN にアソシエートされている VLAN ID。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect アクセス ポイントに VLAN ID を割り当てる例を示します。

```
(Cisco Controller) >config ap flexconnect vlan wlan 192.12.12.1 6 AP02
```

config ap flexconnect web-auth

ローカルでスイッチされる WLAN に外部 Web 認証用 FlexConnect ACL を設定するには、 **config ap flexconnect web-auth** コマンドを使用します。

config ap flexconnect web-auth wlan *wlan_id cisco_ap acl_name* { **enable** | **disable** }

構文の説明

wlan	FlexConnect ACL を設定する無線 LAN を指定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	FlexConnect アクセス ポイントの名前。
acl_name	FlexConnect ACL の名前。
enable	ローカルでスイッチされる無線 LAN に対して FlexConnect ACL をイネーブルにします。
disable	ローカルでスイッチされる無線 LAN に対して FlexConnect ACL をディセーブルにします。

コマンド デフォルト

ローカルでスイッチされる WLAN の外部 Web 認証用 FlexConnect ACL を無効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

AP に固有の FlexConnect ACL のプライオリティは、最も高くなります。WLAN に固有の FlexConnect ACL のプライオリティは、最も低くなります。

次に、WLAN 6 に対して外部 Web 認証用 FlexConnect ACL を有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect web-auth wlan 6 AP2 flexacl2 enable
```

config ap flexconnect web-policy acl

アクセス ポイントに対して Web ポリシー FlexConnect ACL を設定するには、 **config ap flexconnect web-policy acl** コマンドを使用します。

config ap flexconnect web-policy acl {**add** | **delete**} *acl_name*

構文の説明

add	アクセス ポイントに Web ポリシー FlexConnect ACL を追加します。
delete	アクセス ポイントの Web ポリシー FlexConnect ACL を削除します。
acl_name	Web ポリシー FlexConnect ACL の名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントに Web ポリシー FlexConnect ACL を追加する例を示します。

```
(Cisco Controller) >config ap flexconnect web-policy acl add flexacl2
```

config ap flexconnect wlan

ローカルでスイッチされる WLAN の FlexConnect アクセス ポイントを設定するには、**config ap flexconnect wlan** コマンドを使用します。

config ap flexconnect wlan l2acl {**add** *wlan_id cisco_ap acl_name* | **delete** *wlan_id cisco_ap*}

構文の説明

add	FlexConnect アクセス ポイントにレイヤ 2 ACL を追加します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
acl_name	レイヤ 2 ACL の名前。名前には 32 文字以内の英数字を使用できます。
delete	FlexConnect アクセス ポイントからレイヤ 2 ACL を削除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

- レイヤ 2 ACL に対して最大 16 のルールを作成できます。
- Cisco WLC には、最大で 64 の レイヤ 2 ACL を作成できます。
- AP は最大 16 の WLAN をサポートするので、AP ごとに最大 16 のレイヤ 2 ACL がサポートされます。
- AP はレイヤ 2 およびレイヤ 3 の同じ ACL 名をサポートしないため、レイヤ 2 ACL 名が FlexConnect ACL 名と競合していないことを確認します。

次に、FlexConnect AP でレイヤ 2 ACL を設定する例を示します。

```
(Cisco Controller) >config ap flexconnect wlan add 1 AP1600_1 acl_l2_1
```

config ap group-name

Cisco Lightweight アクセス ポイントの内容がわかるグループ名を指定するには、**config ap group-name** コマンドを使用します。

config ap group-name *groupname cisco_ap*

構文の説明

groupname	アクセス ポイント グループの内容がわかる名前。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco Lightweight アクセス ポイントを無効にしてから、このパラメータを変更する必要があります。

次に、アクセス ポイント AP01 の内容がわかる名前を設定する例を示します。

```
(Cisco Controller) >config ap group-name superusers AP01
```

config ap hotspot

アクセス ポイントにホットスポット パラメータを設定するには、**config ap hotspot** コマンドを使用します。

config ap hotspot venue {**type** *group_code type_code* | **name** {**add** *language_code venue_name* | **delete**}} *cisco_ap*

構文の説明

venue	特定の AP グループの場所の情報を設定します。
type	特定の AP グループの場所のタイプを設定します。
group_code	特定の AP グループの場所グループの情報。 次のオプションを使用できます。 • 0：未指定 • 1：アセンブリ • 2：ビジネス • 3：教育 • 4：工場および産業 • 5：機関 • 6：商業 • 7：住居 • 8：倉庫 • 9：公共施設、その他 • 10：乗り物 • 11：アウトドア

type_code

AP グループの場所タイプの情報。

場所グループ 1（集会施設）には、次のオプションが使用できます。

- 0：未指定のアセンブリ
- 1：アリーナ
- 2：スタジアム
- 3：乗客ターミナル
- 4：円形劇場
- 5：アミューズメント パーク
- 6：礼拝所
- 7：会議場
- 8：図書館
- 9：博物館
- 10：レストラン
- 11：シアター
- 12：バー
- 13：喫茶店
- 14：動物園または水族館
- 15：緊急対応センター

場所グループ 2（ビジネス）には、次のオプションが使用できます。

- 0：未指定のビジネス
- 1：医師または歯科医師のオフィス
- 2：銀行
- 3：消防署
- 4：警察署
- 6：郵便局
- 7：専門家のオフィス
- 8：研究および開発施設
- 9：弁護士のオフィス

場所グループ 3（教育施設）には、次のオプションが使用できます。

- 0：未指定の教育機関
- 1：小学校
- 2：中学校
- 3：大学

場所グループ 4（工場および産業）には、次のオプションが使用できます。

- 0：未指定の工場および産業
- 1：工場

場所グループ 5（機関）には、次のオプションが使用できます。

- 0：未指定の公共機関
- 1：病院
- 2：長期看護施設
- 3：アルコールおよび薬物のリハビリテーション センター
- 4：グループ ホーム
- 5:刑務所や拘置所

type_code

場所グループ 6（商業施設）には、次のオプションが使用できます。

- 0：未指定の商業施設
- 1：小売店
- 2：食料品店
- 3：自動車サービス ステーション
- 4：ショッピング モール
- 5：ガソリン スタンド

場所グループ 7（居住施設）には、次のオプションが使用できます。

- 0：未指定の居住施設
- 1：私邸
- 2：ホテルまたはモーテル
- 3：寄宿舎
- 4：宿泊施設

場所グループ 8（倉庫）のオプションは次のとおりです。

- 0：未指定の倉庫

場所グループ 9（公共施設、その他）のオプションは次のとおりです。

- 0：未指定の公共施設およびその他

場所グループ 10（乗り物）には、次のオプションが使用できます。

- 0：未指定の乗り物
- 1：自動車またはトラック
- 2：飛行機
- 3：バス
- 4：フェリー
- 5：船またはボート
- 6：電車
- 7：モーター バイク

場所グループ 11（アウトドア）には、次のオプションが使用できます。

- 0：未指定のアウトドア
- 1：MINI-MESH ネットワーク

- 2：都市公園
- 3：休憩施設
- 4：交通管制施設
- 5：バス停留所
- 6：売店

name	このアクセス ポイントの場所の名前を設定します。
language_code	場所で使用される言語を定義する ISO-639 のコード化文字列。この文字列は 3 文字の言語コードです。たとえば、英語の場合は ENG と入力します。
venue_name	このアクセスポイントの場所の名前。この名前は、基本サービスセット（BSS）に関連付けられ、SSID で場所に関する十分な情報が得られないときに使用されます。場所の名前は最大 252 文字の英数字で、大文字と小文字を区別します。
add	このアクセス ポイントの HotSpot 場所名を追加します。
delete	このアクセス ポイントの HotSpot 場所名を削除します。
cisco_ap	Cisco アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、場所のグループを教育施設として、場所のタイプを大学として設定する例を示します。

```
(Cisco Controller) >config ap hotspot venue type 3 3
```

config ap image predownload

指定したアクセス ポイントにイメージを設定するには、**config ap image predownload** コマンドを使用します。

config ap image predownload {**abort** | **primary** | **backup**} {*cisco_ap* | **all**}

構文の説明

abort	プレダウンロード イメージ・プロセスを中断します。
primary	コントローラのプライマリ・イメージから Cisco アクセス ポイントにイメージをプレダウンロードします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all (Cisco Controller) >	すべてのアクセス ポイントにイメージをプレダウンロードすることを指定します。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、プライマリ イメージからアクセス ポイントにイメージをプレダウンロードする例を示します。

```
(Cisco Controller) >config ap image predownload primary all
```

config ap image swap

アクセス ポイントのプライマリ イメージとバックアップ イメージを切り替えるには、**config ap image swap** コマンドを使用します。

config ap image swap {*cisco_ap* | **all**}

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントに起動イメージを交換することを指定します。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

コマンド デフォルト

なし

次に、アクセスポイントのプライマリおよびセカンダリ イメージを切り替える例を示します。

```
(Cisco Controller) >config ap image swap all
```

config ap lag-mode support

次のコマンドを入力することにより、すべての Cisco Aironet 1850 シリーズ AP または特定の Cisco Aironet 1850 シリーズ AP のリンク集約を設定します。

config ap lag-mode support {**enable** | **disable**} [*ap-name*]

構文の説明

enable	すべての Cisco Aironet 1850 シリーズ AP のリンク集約を有効にします。
disable	すべての Cisco Aironet 1850 シリーズ AP のリンク集約を無効にします。
enable *ap-name*	指定した Cisco Aironet 1850 シリーズ AP のリンク集約を有効にします。
disable *ap-name*	指定した Cisco Aironet 1850 シリーズ AP のリンク集約を無効にします。

コマンド履歴

リリース	変更内容
8.1.110.0	このコマンドが導入されました。

config ap led-state

アクセス ポイントの LED ステートを設定にする場合、または LED の点滅を設定する場合には、**config ap led-state** コマンドを使用します。

config ap led-state {**enable** | **disable**} {*cisco_ap* | **all**}

config ap led-state flash {*seconds* | **indefinite** | **disable**} {*cisco_ap* | **dual-band**}

構文の説明

enable	アクセスポイントのLEDステートを有効にします。
disable	アクセスポイントのLEDステートを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
flash	アクセス ポイントの LED の点滅を設定します。
seconds	LED が点滅している期間。指定できる範囲は 1 ～ 3600 秒です。
indefinite	アクセスポイントのLEDに無制限の点滅を設定します。
dual-band	すべてのデュアルバンドアクセスポイントの LED ステートを設定します。

使用上のガイドライン

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

デュアル バンド無線モジュールを持つアクセス ポイントの LED は、led state flash コマンドを実行する場合に青緑色に点滅します。

コマンド デフォルト

なし

次に、アクセス ポイントの LED ステートを有効にする例を示します。

```
(Cisco Controller) >config ap led-state enable AP02
```

次に、デュアル バンド アクセス ポイントの LED の点滅を有効にする例を示します。

```
(Cisco Controller) >config ap led-state flash 20 dual-band
```

config ap link-encryption

5500 シリーズ コントローラのアクセス ポイントに対して Datagram Transport Layer Security（DTLS）データ暗号化を設定するには、 **config ap link-encryption** コマンドを使用します。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

config ap link-encryption {**enable** | **disable**} {*cisco_ap* | **all**}

構文の説明

enable	アクセス ポイントの DTLS データ暗号化を有効にします。
disable	アクセス ポイントの DTLS データ暗号化を無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントを指定します。

コマンド デフォルト

DTLS データ暗号化は OfficeExtend アクセス ポイントに対しては自動的に有効になりますが、他のすべてのアクセス ポイントに対してはデフォルトで無効になります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

DTLS データ暗号化をサポートするのは Cisco 5500 シリーズのコントローラだけです。この機能は、他のコントローラ プラットフォームでは利用できません。データ暗号化が有効なアクセス ポイントが他のいずれかのコントローラに接続しようとすると、アクセス ポイントはコントローラに接続しますが、データ パケットは暗号化されない状態で送信されます。

DTLS データ暗号化をサポートするのは Cisco 1130、1140、1240、および 1250 シリーズのアクセス ポイントだけであり、データが暗号化されたアクセス ポイントは WPLUS ライセンスがコントローラにインストールされている場合にだけ 5500 シリーズのコントローラに接続できます。WPLUS ライセンスがインストールされていない場合、アクセス ポイントはコントローラに接続できません。

次に、アクセス ポイントのデータ暗号化を有効にする例を示します。

```
(Cisco Controller) >config ap link-encryption enable AP02
```

config ap link-latency

特定のアクセス ポイントまたは現在コントローラにアソシエートされているすべてのアクセス ポイントのリンク遅延を設定するには、**config ap link-latency** コマンドを使用します。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

config ap link-latency {**enable** | **disable** | **reset**} {*cisco_ap* | **all**}

構文の説明

enable	アクセス ポイントのリンク遅延を有効にします。
disable	アクセス ポイントのリンク遅延を無効にします。
reset	すべてのアクセス ポイントのリンク遅延をリセットします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントを指定します。

コマンド デフォルト

リンク遅延は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、現在コントローラに接続されているアクセス ポイントだけに対してリンク遅延を有効または無効にします。将来 join されるアクセス ポイントには適用されません。

次に、すべてのアクセス ポイントのリンク遅延を有効にする例を示します。

```
(Cisco Controller) >config ap link-latency enable all
```

config ap location

Cisco Lightweight アクセス ポイントのロケーション説明を変更するには、**config ap location** コマンドを使用します。

config ap location *location cisco_ap*

構文の説明

location	アクセス ポイントのロケーション名（二重引用符で囲みます）。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

使用上のガイドライン

Cisco Lightweight アクセス ポイントを無効にしてから、このパラメータを変更する必要があります。

次に、アクセス ポイント AP1 のロケーション説明を設定する例を示します。

```
(Cisco Controller) >config ap location "Building 1" AP1
```

config ap logging syslog level

特定のアクセス ポイントまたはすべてのアクセス ポイントに対する syslog メッセージのフィルタリングの重大度レベルを設定するには、**config ap logging syslog level** コマンドを使用します。

config ap logging syslog level *severity_level* {*cisco_ap* | **all**}

構文の説明

severity_level	重大度レベルは次のとおりです。 • 緊急：重大度 0 • アラート：重大度 1 • 重要：重大度 2 • エラー：重大度 3 • 警告：重大度 4 • 通知：重大度 5 • 情報：重大度 6 • デバッグ：重大度 7
cisco_ap	シスコ アクセス ポイント。
all	すべてのアクセス ポイントを指定します。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

コマンド デフォルト

なし

使用上のガイドライン

syslog レベルを設定する場合は、重大度がそのレベル以下のメッセージだけがアクセスポイントに送信されます。たとえば、syslog レベルを警告（重大度 4）に設定した場合は、重大度が 0 ～ 4 のメッセージだけがアクセス ポイントに送信されます。

次に、syslog メッセージのフィルタリングの重大度を 3 に設定する例を示します。

```
(Cisco Controller) >config ap logging syslog level 3
```

config ap logging syslog facility

特定のアクセス ポイントまたはすべてのアクセス ポイントに対する syslog メッセージのフィルタリングのファシリティ レベルを設定するには、**config ap logging syslog facility** コマンドを使用します。

config ap logging syslog facility *facility-level* {*cisco_ap* | **all**}

構文の説明

facility-level	ファシリティ レベルは次のいずれかです。 • auth = 認証システム。 • cron = cron/at ファシリティ。 • daemon = システム デーモン。 • kern = カーネル。 • local0 = ローカル使用。 • local1 = ローカル使用。 • local2 = ローカル使用。 • local3 = ローカル使用。 • local4 = ローカル使用。 • local5 = ローカル使用。 • local5 = ローカル使用。 • local6 = ローカル使用。 • local7 = ローカル使用。 • lpr = ライン プリンタ システム。 • mail = メール システム。 • news = USENET ニュース。 • sys10 = システム使用。 • sys11 = システム使用。 • sys12 = システム使用。 • sys13 = システム使用。 • sys14 = システム使用。 • sys9 = システム使用。 • syslog = Syslog 自体。 • user = ユーザ プロセス。 • uucp = UNIX 間コピー システム。
cisco_ap	特定のアクセスポイントに対して設定します。
all	すべてのアクセス ポイントに対して設定します。

コマンド デフォルト

なし

次に、すべてのアクセス ポイントに対する syslog メッセージのフィルタリングのフィルタリング レベルを auth に設定する例を示します。

```
(Cisco Controller) >config ap logging syslog facility auth all
```

config ap max-count

Cisco Wireless LAN Controller（WLC）でサポートされるアクセス ポイントの最大数を設定するには、**config ap max-count** コマンドを使用します。

config ap max-count *number*

構文の説明

number	Cisco WLC でサポートされるアクセス ポイントの数。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

設定された値がライセンスのアクセス ポイント数を超えている場合、Cisco WLC ライセンスのアクセス ポイント数がこの数よりも優先されます。値が 0 の場合は、アクセス ポイントの最大数に制限がなくなります。高可用性が設定されている場合は、Cisco WLC でサポートされるアクセス ポイントの最大数を設定した後に、アクティブ Cisco WLC とスタンバイ Cisco WLC の両方を再起動する必要があります。

次に、Cisco WLC でサポートされるアクセス ポイントの数を設定する例を示します。

```
(Cisco Controller) >config ap max-count 100
```

config ap mgmtuser add

AP 管理用のユーザ名、パスワード、シークレット パスワードを設定するには、 **config ap mgmtuser add** コマンドを使用します。

config ap mgmtuser add username *AP_username* **password** *AP_password* **secret** *secret* {**all** | *cisco_ap*}

構文の説明

username	AP 管理用のユーザ名を設定します。
AP_username	管理ユーザ名。
password	AP 管理用のパスワードを設定します。
AP_password	AP 管理パスワード。
secret	特権 AP 管理用のシークレット パスワードを設定します。
secret	AP 管理シークレット パスワード。
all	特定のユーザ名がないすべての AP に設定を適用します。
cisco_ap	シスコ アクセス ポイント。

コマンド デフォルト

なし

使用上のガイドライン

パスワードについて、次の要件が実施されます。

- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。
- パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
- パスワードには、管理ユーザ名やユーザ名を逆にしたものを使用しないでください。
- パスワードに使用しないほうがよい文字には、Cisco、oscic、admin、nimda のような語のほか、大文字の代わりに 1 や |、！を、o の代わりに 0 を、s の代わりに $ を使用して置き換えた文字などがあります。

シークレット パスワードについて、次の要件が実施されます。

- シークレット パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。

次に、AP 管理用のユーザ名、パスワード、シークレット パスワードを追加する例を示します。

```
(Cisco Controller) > config ap mgmtuser add username acd password Arc_1234 secret Mid_45
 all
```

config ap mgmtuser delete

特定のアクセス ポイントがコントローラのグローバル クレデンシャルを使用するように強制するには、**config ap mgmtuser delete** コマンドを使用します。

config ap mgmtuser delete *cisco_ap*

構文の説明

cisco_ap	アクセス ポイント。

コマンド デフォルト

なし

次に、アクセス ポイントのクレデンシャルを削除する例を示します。

```
(Cisco Controller) > config ap mgmtuser delete cisco_ap1
```

config ap mode

個別の Cisco Lightweight アクセス ポイントの Cisco WLC 通信オプションを変更するには、**config ap mode** コマンドを使用します。

config ap mode {**bridge** | **flexconnect submode** {**none** | **wips** | **pppoe-only** | **pppoe-wips**} | **local submode** {**none** | **wips**} | **reap** | **rogue** | **sniffer** | **se-connect** | **monitor submode** {**none** | **wips**} | **flex+bridge submode**{**none** | **wips** | **pppoe-only** | **pppoe-wips**} } *cisco_ap*

構文の説明

bridge	Lightweight アクセス ポイントからメッシュ アクセス ポイント（ブリッジモード）に変換します。
flexconnect	アクセス ポイントで FlexConnect モードを有効にします。
local	屋内メッシュ アクセス ポイント（MAP または RAP）から nonmesh Lightweight アクセス ポイント（ローカル モード）に変換します。
reap	アクセス ポイントでリモート エッジ アクセス ポイント モードを有効にします。
rogue	アクセス ポイントで有線の不正なアクセス ポイントの検出モードを有効にします。
sniffer	アクセス ポイントで無線スニファ モードを有効にします。
se-connect	アクセス ポイントで Flex + ブリッジ モードを有効にします。
flex+bridge	アクセス ポイントで Spectrum Expert モードを有効にします。
submode	（任意）アクセス ポイントで wIPS サブモードを設定します。
none	アクセス ポイントで wIPS を無効にします。
wips	アクセス ポイントで wIPS サブモードを有効にします。
pppoe-only	アクセス ポイントで PPPoE サブモードを有効にします。

pppoe-wips	アクセス ポイントで PPPoE-wIPS サブモードを有効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

ローカル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	**flex+bridge** キーワードが追加されました。

使用上のガイドライン

スニファ モードは、そのチャネル上のクライアントからすべてのパケットを取得し、Airopeek を実行するリモート マシンまたはその他のサポート対象パケット アナライザ ソフトウェアに転送します。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

次に、ブリッジ モードでアクセス ポイント AP91 と通信するようにコントローラを設定する例を示します。

```
(Cisco Controller) > config ap mode bridge AP91
```

次に、ローカル モードでアクセス ポイント AP01 と通信するようにコントローラを設定する例を示します。

```
(Cisco Controller) > config ap mode local AP01
```

次に、リモート オフィス（REAP）モードでアクセス ポイント AP91 と通信するようにコントローラを設定する例を示します。

```
(Cisco Controller) > config ap mode flexconnect AP91
```

次に、有線の不正なアクセス ポイントの検出モードでアクセス ポイント AP91 と通信するようにコントローラを設定する例を示します。

```
(Cisco Controller) > config ap mode rogue AP91
```

次に、無線スニファ モードでアクセス ポイント AP02 と通信するようにコントローラを設定する例を示します。

```
(Cisco Controller) > config ap mode sniffer AP02
```

config ap module3g

Cisco Universal Small Cell（USC）8x18 デュアルモード モジュールを設定するには、**config ap module3g** コマンドを使用します。

config ap module3g {**enable** | **disable**} *ap-name*

構文の説明

enable	指定した Cisco AP で Cisco USC 8x18 デュアル モード モジュールを有効にします。
disable	指定した Cisco AP で Cisco USC 8x18 デュアル モード モジュールを無効にします。
ap-name	Cisco AP の名前。 （注） リリース 8.1 では、Cisco Aironet 3600I および 3700I AP のみがサポートされています。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

使用上のガイドライン

2.4 GHz の Wi-Fi と 3G/4G モジュールを有効にすると、共存の警告が表示される場合があります。

次に、*my-ap* という Cisco AP で Cisco USC 8x18 デュアル モード モジュールを有効にする例を示します。

```
(Cisco Controller) >config ap module3g enable my-ap
```

config ap monitor-mode

Cisco Lightweight アクセス ポイント チャネルの最適化を設定するには、**config ap monitor-mode** コマンドを使用します。

config ap monitor-mode {**802.11b fast-channel** | **no-optimization** | **tracking-opt** | **wips-optimized**} *cisco_ap*

構文の説明

802.11b fast-channel	監視モードアクセス ポイントに対して 802.11b スキャン チャネルを設定します。
no-optimization	アクセス ポイントに対してチャネル スキャンの最適化を行わないことを指定します。
tracking-opt	アクセス ポイントに対してトラッキングが最適化されたチャネル スキャンを有効にします。
wips-optimized	アクセス ポイントに対して wIPS が最適化されたチャネル スキャンを有効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

次に、アクセス ポイント AP01 に Cisco wireless Intrusion Prevention System（wIPS）監視モードを設定する例を示します。

```
(Cisco Controller) > config ap monitor-mode wips-optimized AP01
```

config ap name

Cisco Lightweight アクセス ポイントの名前を変更するには、**config ap name** コマンドを使用します。

config ap name *new_name old_name*

構文の説明

new_name	Cisco Lightweight アクセス ポイントの新しい名前。
old_name	Cisco Lightweight アクセス ポイントの現在の名前。

コマンド デフォルト

なし

次に、アクセス ポイントの名前を AP1 から AP2 に変更する例を示します。

```
(Cisco Controller) > config ap name AP1 AP2
```

config ap packet-dump

アクセス ポイントのパケット キャプチャ パラメータを設定するには、**config ap packet-dump** コマンドを使用します。

config ap packet-dump {**buffer-size** *Size _in_KB* | **capture-time** *Time_in_Min* | **ftp serverip** *IP_addr* **path** *path* **username** *username***password** *password* | **start** *MAC_address Cisco_AP* | **stop** | **truncate** *Length_in_Bytes*}
config ap packet-dump classifier {{**arp** | **broadcast** | **control** | **data** | **dot1x** | **iapp** | **ip** | **management** | **multicast** } {**enable** | **disable**} | **tcp** {**enable** | **disable** | **port** *TCP_Port* {**enable** | **disable**}} | **udp** {**enable** | **disable** | **port** *UDP_Port* {**enable** | **disable**}}}

構文の説明

buffer-size	アクセス ポイントにパケット キャプチャのバッファ サイズを設定します。
Size _in_KB	バッファのサイズ。指定できる範囲は 1024 ～ 4096 KB です。
capture-time	パケット キャプチャのタイマー値を設定します。
Time_in_Min	パケット キャプチャのタイマー値。範囲は 1 ～ 60 分です。
ftp	パケット キャプチャの FTP パラメータを設定します。
serverip	FTP サーバを設定します。
IP_addr	FTP サーバの IP アドレスです。
path *path*	FTP サーバのパスを設定します。
username *user_ID*	FTP サーバ用のユーザ名を設定します。
password *password*	FTP サーバ用のパスワードを設定します。
start	アクセス ポイントからパケット キャプチャを開始します。

MAC_address	パケット キャプチャのクライアントの MAC アドレス。
Cisco_AP	Cisco アクセス ポイントの名前。
stop	アクセス ポイントからパケット キャプチャを停止します。
truncate	パケット キャプチャ中にパケットを指定の長さに切り捨てます。
Length_in_Bytes	切り捨て後のパケットの長さ。範囲は 20 ～ 1500 です。
classifier	パケット キャプチャの分類子情報を設定します。キャプチャ対象とする必要のあるパケットのタイプを指定できます。
arp	ARP パケットをキャプチャします。
enable	ARP、ブロードキャスト、802.11 制御、802.11 データ、dot1x、Inter Access Point Protocol（IAPP）、IP、802.11 管理、またはマルチキャスト パケットのキャプチャを有効にします。
disable	ARP、ブロードキャスト、802.11 制御、802.11 データ、dot1x、IAPP、IP、802.11 管理、またはマルチキャスト パケットのキャプチャを無効にします。
broadcast	ブロードキャスト パケットをキャプチャします。
control	802.11 制御パケットをキャプチャします。
data	802.11 データ パケットをキャプチャします。

dot1x	dot1x パケットをキャプチャします。
iapp	IAPP パケットをキャプチャします。
ip	IP パケットをキャプチャします。
management	802.11 管理パケットをキャプチャします。
multicast	マルチキャスト パケットをキャプチャします。
tcp	TCP パケットをキャプチャします。
TCP_Port	TCP ポート番号。有効な範囲は 1 ～ 65535 です。
udp	TCP パケットをキャプチャします。
UDP_Port	UDP ポート番号。有効な範囲は 1 ～ 65535 です。
ftp	パケット キャプチャの FTP パラメータを設定します。
server_ip	FTP サーバの IP アドレス。

コマンド デフォルト

デフォルトのバッファ サイズは 2 MB です。デフォルトのキャプチャ時間は 10 分です。

使用上のガイドライン

コントローラ間ローミング中には、パケット キャプチャは機能しません。

コントローラでは、ビーコンやプローブの応答など、無線ファームウェアに作成され、アクセス ポイントから送信されたパケットをキャプチャしません。Tx パスで無線ドライバを通過するパケットだけがキャプチャされます。

config ap packet-dump start コマンドを使用して、アクセス ポイントからパケット キャプチャを開始します。パケット キャプチャを開始すると、コントローラは、クライアントがアソシエートされるアクセス ポイントに Control and Provisioning of Wireless Access Points（CAPWAP）メッセージを送信し、パケットをキャプチャします。パケット キャプチャを開始する前に、FTP サーバを設定し、クライアントがアクセス ポイントにアソシエートされている必要があります。クライアントがアクセス ポイントにアソシエートされていない場合、アクセス ポイントの名前を指定する必要があります。

このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、アクセス ポイントからパケット キャプチャを開始する例を示します。

```
(Cisco Controller) >config ap packet-dump start 00:0d:28:f4:c0:45 AP1
```

次に、アクセス ポイントから 802.11 制御パケットをキャプチャする例を示します。

```
(Cisco Controller) >config ap packet-dump classifier control enable
```

config ap port

外部アクセス ポイントのポートを設定するには、**config ap port** コマンドを使用します。

config ap port *MAC port*

構文の説明

MAC	外部アクセス ポイントの MAC アドレス。
port	外部アクセス ポイントにアクセスするポート番号。

コマンド デフォルト

なし

次に、外部アクセス ポイントの MAC アドレスのポートを設定する例を示します。

```
(Cisco Controller) > config ap port 12:12:12:12:12:12 20
```

config ap power injector

アクセス ポイントのパワー インジェクタ ステートを設定するには、**config ap power injector** コマンドを使用します。

config ap power injector {**enable** | **disable**} {*cisco_ap* | **all**} {**installed** | **override** | *switch_MAC*}

構文の説明

enable	アクセス ポイントのパワー インジェクタ ステートを有効にします。
disable	アクセス ポイントのパワー インジェクタ ステートを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	コントローラに接続されたすべての Cisco Lightweight アクセス ポイントを指定します。
installed	パワーインジェクタが設置された現在のスイッチ ポートの MAC アドレスを検出します。
override	安全性チェックを上書きし、パワー インジェクタが常にインストールされていることを前提とします。
switch_MAC	パワー インジェクタが設置されたスイッチ ポートの MAC アドレス。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

コマンド デフォルト

なし

次に、すべてのアクセス ポイントのパワー インジェクタ ステートを有効にする例を示します。

```
(Cisco Controller) > config ap power injector enable all 12:12:12:12:12:12
```

config ap power pre-standard

アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効または無効にするには、**config ap power pre-standard** コマンドを使用します。

config ap power pre-standard {**enable** | **disable**} *cisco_ap*

構文の説明

enable	アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にします。
disable	アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

ディセーブル

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にする例を示します。

```
(Cisco Controller) > config ap power pre-standard enable AP02
```

config ap preferred-mode

優先モードを設定するには、**config ap preferred-mode** コマンドを使用します。

config appreferred-mode{**ipv4** | **ipv6**|**any**}{*AP_name* | *Ap-group_name* | *all* }

構文の説明

ipv4	IPv4 を優先モードに設定します。
ipv6	IPv6 を優先モードに設定します。
any	any を優先モードに設定します。
AP_name	AP に優先モードを設定します。
Ap-group_name	AP グループのメンバーに優先モードを設定します。
all	すべての AP に優先モードを設定します。

コマンド デフォルト

なし

例

次に、Lightweight アクセス ポイント AP1 に対して IPv6 を優先モードに設定する例を示します。

```
(Cisco Controller) >config ap preferred-mode ipv6 AP1
```

config ap primary-base

Cisco Lightweight アクセス ポイントのプライマリ Cisco WLC を設定するには、**config ap primary-base** コマンドを使用します。

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

構文の説明

controller_name	Cisco WLC の名前。
Cisco_AP	Cisco Lightweight アクセス ポイント名。
controller_ip_address	（任意）アクセスポイントの接続先モビリティ グループの外部にバックアップ コントローラが配置されている場合は、プライマリ、セカンダリ、またはターシャリ コントローラの IP アドレスを指定する必要があります。 （注） OfficeExtend アクセス ポイントの場合は、コントローラに対して名前と IP アドレスの両方を入力する必要があります。入力しないと、アクセス ポイントはコントローラに join できません。

コマンド デフォルト

なし

使用上のガイドライン

Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco WLC と関連付けられます。

OfficeExtend アクセス ポイントは、コントローラを見つけるために一般的なブロードキャストまたは無線（OTAP）検出プロセスを使用しません。OfficeExtend アクセス ポイントは設定されたコントローラにだけ接続しようとするため、1 つまたは複数のコントローラを設定する必要があります。

このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、Cisco AP のアクセス ポイントのプライマリ Cisco WLC IPv4 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap primary-base SW_1 AP2 10.0.0.0
```

次に、Cisco AP のアクセス ポイントのプライマリ Cisco WLC IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap primary-base SW_1 AP2 2001:DB8:0:1::1
```

関連コマンド **show ap config general**

config ap priority

アクセスポイントに優先度を割り当ててコントローラの障害発生後に早い順ではなく優先度に従ってアクセス ポイントの再認証を行うには、**config ap priority** コマンドを使用します。

config ap priority {**1** | **2** | **3** | **4**} *cisco_ap*

構文の説明

1	低優先度を指定します。
2	中間の優先度を指定します。
3	高プライオリティを指定します。
4	最高（クリティカル）の優先度を指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

1：低い優先度。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

フェールオーバーの状況では、影響を受ける領域内のすべてのアクセス ポイントを再認証するのに十分なポートがバックアップ コントローラに存在しない場合に、低い優先度のアクセス ポイントよりも高い優先度のアクセス ポイントが優先されます（これは低い優先度のアクセス ポイントを置き換える場合であっても同様です）。

次に、アクセス ポイント AP02 に優先度を割り当ててコントローラの障害発生後に再認証優先度 3 を割り当てることによって、アクセス ポイントを再認証する例を示します。

```
(Cisco Controller) > config ap priority 3 AP02
```

config ap reporting-period

Cisco Lightweight アクセス ポイントをリセットするには、**config ap reporting-period** コマンドを使用します。

config ap reporting-period *period*

構文の説明

period	10 ～ 120 秒の期間。

コマンド デフォルト

なし

次に、120 秒にアクセス ポイント レポート期間をリセットする例を示します。

```
> config ap reporting-period 120
```

config ap reset

Cisco Lightweight アクセス ポイントをリセットするには、**config ap reset** コマンドを使用します。

config ap reset *cisco_ap*

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、アクセス ポイントをリセットする例を示します。

```
(Cisco Controller) > config ap reset AP2
```

config ap retransmit interval

アクセス ポイントで制御パケットの再送信間隔を設定するには、**config ap retransmit interval** コマンドを使用します。

config ap retransmit interval *seconds* {**all** | *cisco_ap*}

構文の説明

seconds	2～5 秒の AP 制御パケットの再送信タイムアウト。
all	すべてのアクセス ポイントを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、すべてのアクセス ポイントの再送信の間隔をグローバルに設定する例を示します。

```
(Cisco Controller) > config ap retransmit interval 4 all
```

config ap retransmit count

アクセス ポイントで制御パケットの再送信回数を設定するには、**config ap retransmit count** コマンドを使用します。

config ap retransmit count *count* {**all** | *cisco_ap*}

構文の説明

count	制御パケットが再送信される回数。範囲は 3 ～ 8 です。
all	すべてのアクセス ポイントを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、特定のアクセス ポイントに対する再送信の再試行回数を設定する例を示します。

```
(Cisco Controller) > config ap retransmit count 6 cisco_ap
```

config ap role

メッシュ ネットワーク内のアクセス ポイントのロールを指定するには、**config ap role** コマンドを使用します。

config ap role {**rootAP** | **meshAP**} *cisco_ap*

構文の説明

rootAP	ルート アクセス ポイント（RAP）としてメッシュ アクセス ポイントを指定します。
meshAP	メッシュ アクセス ポイント（MAP）としてメッシュ アクセス ポイントを指定します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

meshAPを使用して無効にすることができます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

アクセス ポイントでコントローラに対して無線接続が存在する場合は **meshAP** キーワード、アクセス ポイントでコントローラに対して有線接続が存在する場合は **rootAP** キーワードを使用します。AP のロールを変更すると、AP が再起動します。

次に、ルート アクセス ポイントとしてメッシュ アクセス ポイント AP02 を指定する例を示します。

```
(Cisco Controller) > config ap role rootAP AP02
Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

config ap rst-button

アクセス ポイントの Reset ボタンを設定するには、**config ap rst-button** コマンドを使用します。

config ap rst-button {**enable** | **disable**} *cisco_ap*

構文の説明

enable	アクセス ポイントの Reset ボタンを有効にします。
disable	アクセス ポイントの Reset ボタンを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイント AP03 の Reset ボタンを設定する例を示します。

```
(Cisco Controller) > config ap rst-button enable AP03
```

config ap secondary-base

Cisco Lightweight アクセス ポイントのセカンダリ Cisco WLC を設定するには、 **config ap secondary-base** コマンドを使用します。

config ap secondary-base *Controller_name Cisco_AP*［*Controller_IP_address*］

構文の説明

controller_name	Cisco WLC の名前。
Cisco_AP	Cisco Lightweight アクセス ポイント名。
Controller_IP_address	（任意）。アクセス ポイントの接続先モビリティ グループの外部にバックアップ Cisco WLC が配置されている場合は、プライマリ、セカンダリ、またはターシャリ Cisco WLC の IP アドレスを指定する必要があります。 （注） OfficeExtend アクセス ポイントの場合は、Cisco WLC に対して名前と IP アドレスの両方を入力する必要があります。入力しないと、アクセス ポイントはこの Cisco WLC に join できません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco WLC と関連付けられます。

OfficeExtend アクセス ポイントは、Cisco WLC を見つけるために一般的なブロードキャストまたは無線（OTAP）検出プロセスを使用しません。OfficeExtend アクセス ポイントは設定された Cisco WLC にだけ接続しようとするため、1 つまたは複数の Cisco WLC を設定する必要があります。

このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、アクセス ポイントのセカンダリ Cisco WLC を設定する例を示します。

```
(Cisco Controller) > config ap secondary-base SW_1 AP2 10.0.0.0
```

次に、Cisco AP のアクセス ポイントのプライマリ Cisco WLC IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap secondary-base SW_1 AP2 2001:DB8:0:1::1
```

関連コマンド

show ap config general

config ap slub-debug

アクセス ポイントでの slub デバッグを設定するには、**config ap slub-debug** コマンドを使用します。

（注）

config ap slub-debug {**sanity** | **red-zoning** | **poisoning** | **user-tracking** | **disable**} *cisco_ap* | **all**

構文の説明

sanity	健全性 slub デバッグ モードを設定します。
red-zoning	レッドゾーン化 slub デバッグ モードを設定します。
poisoning	ポイズニング slub デバッグ モードを設定します。
user-tracking	ユーザ トラッキング slub デバッグ モードを設定します。
disable	slub デバッグ モードを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべての Cisco アクセス ポイントに適用されます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.2.160.0	このコマンドが導入されました。

使用上のガイドライン

有効/無効になる場合または slub デバッグ機能のモードを切り替える場合は、Cisco AP が再起動します。

次に、すべての Cisco AP で slub デバッグを無効にする例を示します。

```
(Cisco Controller) >config ap slub-debug disable all

Changing the AP's slub debug mode will cause the AP to reboot.
Are you sure you want to continue? (y/n) n
```

```
Slub debug mode not changed!
(Cisco Controller) >
```

config ap sniff

アクセス ポイントでスニフィングを有効または無効にするには、**config ap sniff** コマンドを使用します。

config ap sniff {**802.11a** | **802.11b**} {**enable** *channel server_ip* | **disable**} *cisco_ap*

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
enable	アクセス ポイントでスニフィングを有効にします。
channel	スニファ対象チャネル。
server_ip	Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレス。
disable	アクセス ポイントでスニフィングを無効にします。
cisco_ap	スニファとして設定されたアクセスポイント。

コマンド デフォルト

チャネル 36。

使用上のガイドライン

アクセス ポイントでスニフィング機能が有効になっている場合、そのアクセス ポイントは指定されたチャネルで信号のスニフィングを開始します。すべてのパケットが取得され、Omnipeek、Airopeek、AirMagnet、または Wireshark ソフトウェアを実行しているリモート コンピュータに転送されます。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

アクセスポイントをスニファとして機能させるには、そのアクセスポイントが送信したパケットを、上記いずれかのパケット アナライザを実行しているリモート コンピュータが受信できるように設定しておく必要があります。Airopeek のインストール後、次の .dll ファイルを Airopeek がインストールされている場所にコピーします。

- socket.dll ファイルを Plug-ins フォルダにコピーします（C:\Program Files\WildPackets\AiroPeek\Plugins など）
- socketres.dll ファイルを PluginRes フォルダにコピーします（C:\Program Files\WildPackets\AiroPeek\ 1033\PluginRes など）

次に、802.11a アクセス ポイントでのスニフィングをプライマリ Cisco WLC から有効にする例を示します。

```
(Cisco Controller) > config ap sniff 80211a enable 23 11.22.44.55 AP01
```

config ap ssh

アクセス ポイントで Secure Shell（SSH）接続を有効にするには、**config ap ssh** コマンドを使用します。

config ap ssh {**enable** | **disable** | **default**} *cisco_ap* | *all*

構文の説明

enable	アクセス ポイントで SSH 接続を有効にします。
disable	アクセス ポイントで SSH 接続を無効にします。
default	アクセス ポイントの特定の SSH 設定をグローバル SSH 設定で置き換えます。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべてのアクセス ポイント。

コマンド デフォルト

なし

使用上のガイドライン

Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco ワイヤレス LAN コントローラと関連付けられます。

次に、アクセス ポイント Cisco_ap2 で SSH 接続を有効にする例を示します。

```
> config ap ssh enable cisco_ap2
```

config ap static-ip

Cisco Lightweight アクセス ポイントの静的 IP アドレスを設定するには、**config ap static-ip** コマンドを使用します。

config ap static-ip {**enable** *Cisco_AP AP_IP_addr IP_netmask /prefix_length gateway* | **disable** *Cisco_AP* | **add** {**domain** {*Cisco_AP* | **all**} *domain_name* | **nameserver** {*Cisco_AP* | **all**} *nameserver-ip*} | **delete** {**domain** | **nameserver**} {*Cisco_AP* | **all**}}

構文の説明

enable	Cisco Lightweight アクセス ポイントの静的 IP アドレスを有効にします。
disable	Cisco Lightweight アクセス ポイントの静的 IP アドレスを無効にします。その場合、アクセス ポイントは DHCP を使用して IP アドレスを取得します。
Cisco_AP	Cisco Lightweight アクセス ポイント名。
AP_IP_addr	Cisco Lightweight アクセス ポイントの IP アドレス。
IP_netmask/prefix_length	Cisco Lightweight アクセス ポイントのネットワーク マスク。
gateway	Cisco Lightweight アクセス ポイント ゲートウェイの IP アドレス。
add	ドメインまたは DNS サーバを追加します。
domain	特定のアクセス ポイントまたはすべてのアクセスポイントが属するドメインを指定します。
all	すべてのアクセス ポイントを指定します。
domain_name	ドメイン名を指定します。
nameserver	特定のアクセス ポイントまたはすべてのアクセス ポイントが DNS 解決を使用してコントローラを検出できるよう DNS サーバを指定します。
nameserver-ip	DNS サーバの IP アドレス。
delete	ドメインまたは DNS サーバを削除します。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

コマンド デフォルト

なし

使用上のガイドライン

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバとアクセス ポイントが属するドメインを指定しない限り、アクセスポイントはドメイン ネーム システム（DNS）解決を使用してコントローラを検出できません。

IPv6 アドレス、プレフィックス長、および IPv6 ゲートウェイ アドレスの を入力すると、アクセス ポイント用に CAPWAP トンネルが再起動します。AP の IP アドレスを変更すると、AP の接続が解除されます。アクセス ポイントのコントローラへの再接続後、ドメインと IPv6 DNS サーバ情報を入力できます。

このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、アクセス ポイントの静的 IP アドレスを設定する例を示します。

```
(Cisco Controller) >config ap static-ip enable AP2 209.165.200.225 255.255.255.0
209.165.200.254
```

次に、アクセス ポイントの静的 IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap static-ip enable AP2 2001:DB8:0:1::1
```

関連コマンド

show ap config general

config ap stats-timer

Cisco Lightweight アクセス ポイントが Cisco ワイヤレス LAN コントローラに DOT11 統計情報を送信する時間（秒単位）を設定するには、**config ap stats-timer** コマンドを使用します。

config ap stats-timer *period cisco_ap*

構文の説明

period	0 ～ 65535 の時間（秒単位）。ゼロの値を指定すると、タイマーが無効になります。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

デフォルト値は 0（無効状態）です。

使用上のガイドライン

値 0 は、Cisco Lightweight アクセス ポイントが DOT11 統計情報を送信しないことを意味します。このタイマーには 0 ～ 65,535 秒を指定できます。Cisco Lightweight アクセス ポイントを無効にしてから、この値を設定する必要があります。

次に、アクセス ポイント AP2 で、統計情報タイマーを 600 秒に設定する例を示します。

```
(Cisco Controller) > config ap stats-timer 600 AP2
```

config ap syslog host global

コントローラに結合されているアクセス ポイントすべてのグローバル syslog サーバを設定するには、**config ap syslog host global** コマンドを使用します。

config ap syslog host global *ip_address*

構文の説明

ip_address	syslog サーバの IPv4/IPv6 アドレス。

コマンド デフォルト

syslog サーバの IPv4 アドレスのデフォルト値は 255.255.255.255 です。

使用上のガイドライン

デフォルトでは、すべてのアクセス ポイントのグローバル syslog サーバ IP アドレスは 255.255.255.255 です。コントローラ上の syslog サーバを設定する前に、アクセス ポイントがこのサーバが常駐するサブネットにアクセスできることを確認します。このサブネットにアクセスできない場合、アクセス ポイントは syslog メッセージを送信できません。

このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、IPv4 アドレスを使用してすべてのアクセス ポイントにグローバル syslog サーバを設定する例を示します。

```
(Cisco Controller) > config ap syslog host global 255.255.255.255
```

次に、IPv6 アドレスを使用してすべてのアクセス ポイントにグローバル syslog サーバを設定する例を示します。

```
(Cisco Controller) > config ap syslog host global  2001:9:10:56::100
```

config ap syslog host specific

特定のアクセス ポイントの syslog サーバを設定するには、**config ap syslog host specific** コマンドを使用します。

config ap syslog host specific *ap_nameip_address*

構文の説明

ap_name	Cisco Lightweight アクセス ポイント。
ip_address	syslog サーバの IPv4/IPv6 アドレス。

コマンド デフォルト

syslog サーバの IP アドレスのデフォルト値は 0.0.0.0 です。

使用上のガイドライン

デフォルトでは、各アクセス ポイントの syslog サーバ IP アドレスは 0.0.0.0 で、これはまだサーバが設定されていないことを示しています。このデフォルト値を使用すると、グローバル アクセス ポイント syslog サーバの IP アドレスがアクセス ポイントにプッシュされます。

このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、Syslog サーバを設定する例を示します。

```
(Cisco Controller) >config ap syslog host specific 0.0.0.0
```

次に、IPv6 アドレスを使用して特定の AP に syslog サーバを設定する例を示します。

```
(Cisco Controller) > config ap syslog host specific AP3600 2001:9:10:56::100
```

config ap tcp-mss-adjust

特定のアクセス ポイントまたはすべてのアクセス ポイントで TCP 最大セグメント サイズ（MSS）を有効または無効にするには、**config ap tcp-mss-adjust** コマンドを使用します。

config ap tcp-mss-adjust {**enable** | **disable**} {*cisco_ap* | **all**} *size*

構文の説明

enable	アクセス ポイントで TCP 最大セグメント サイズを有効にします。
disable	アクセス ポイントで TCP 最大セグメント サイズを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべてのアクセス ポイントを指定します。
size	最大セグメント サイズ。 • IPv4：536 ～ 1363 の値を指定します。 • IPv6：1220 ～ 1331 の値を指定します。 （注） CAPWAP v6 AP では、1220 未満または 1331 より大きい TCP MSS 値は無効です。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

コマンド デフォルト

なし

使用上のガイドライン

この機能を有効にすると、アクセス ポイントがデータ パスの無線クライアントへの TCP パケットとデータ パスの無線クライアントからの TCP パケットをチェックします。これらのパケットの MSS が設定した値または CAPWAP トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。

次に、セグメント サイズが 1200 バイトであるアクセス ポイント cisco_ap1 で TCP MSS を有効にする例を示します。

```
(Cisco Controller) > config ap tcp-mss-adjust enable cisco_ap1 1200
```

config ap telnet

アクセス ポイントで Telnet 接続を有効にするには、**config ap telnet** コマンドを使用します。

config ap telnet {**enable** | **disable** | **default**} *cisco_ap* | *all*

構文の説明

enable	アクセス ポイントで Telnet 接続を有効にします。
disable	アクセス ポイントで Telnet 接続を無効にします。
default	アクセス ポイントの特定の Telnet 設定をグローバル Telnet 設定に置き換えます。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべてのアクセス ポイント。

コマンド デフォルト

なし

使用上のガイドライン

- Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco WLC と関連付けられます。
- Telnet は、Cisco Aironet 1810 OEAP、1810W、1830、1850、2800、および 3800 シリーズの AP ではサポートされていません。

次に、アクセス ポイント cisco_ap1 で Telnet 接続を有効にする例を示します。

```
(Cisco Controller) >config ap telnet enable cisco_ap1
```

次に、アクセス ポイント cisco_ap1 で Telnet 接続を無効にする例を示します。

```
(Cisco Controller) > config ap telnet disable cisco_ap1
```

config ap tertiary-base

Cisco Lightweight アクセス ポイントのターシャリ Cisco WLC を設定するには、**config ap tertiary-base** コマンドを使用します。

config ap tertiary-base *controller_name Cisco_AP*［*controller_ip_address*］

構文の説明

controller_name	Cisco WLC の名前。
Cisco_AP	Cisco Lightweight アクセス ポイント名。
controller_ip_address	（任意）アクセスポイントの接続先モビリティ グループの外部にバックアップ コントローラが配置されている場合は、プライマリ、セカンダリ、またはターシャリ Cisco WLC の IP アドレスを指定する必要があります。 （注） OfficeExtend アクセス ポイントの場合は、Cisco WLC に対して名前と IP アドレスの両方を入力する必要があります。入力しないと、アクセスポイントはこの Cisco WLC に join できません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

OfficeExtend アクセス ポイントは、Cisco WLC を見つけるために一般的なブロードキャストまたは無線（OTAP）検出プロセスを使用しません。OfficeExtend アクセス ポイントは設定された Cisco WLC にだけ接続しようとするため、1 つまたは複数のコントローラを設定する必要があります。

Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco WLC と関連付けられます。

このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、アクセス ポイントのターシャリ Cisco WLC を設定する例を示します。

```
(Cisco Controller) > config ap tertiary-base SW_1 AP02 10.0.0.0
```

次に、Cisco AP のアクセス ポイントのターシャリ Cisco WLC IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap tertiary-base SW_1 AP2 2001:DB8:0:1::1
```

関連コマンド

show ap config general

config ap tftp-downgrade

Lightweight アクセス ポイントを Autonomous アクセス ポイントにダウングレードするために使用される設定を指定するには、**config ap ftp-downgrade** コマンドを使用します。

config ap tftp-downgrade *tftp_ip_addressfilename Cisco_AP*

構文の説明

tftp_ip_address	TFTP サーバの IP アドレスです。
filename	TFTP サーバ上のアクセス ポイント イメージ ファイルのファイル名。
Cisco_AP	アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、アクセス ポイント ap1240_102301 をダウングレードするための設定方法を示します。

```
(Cisco Controller) >config ap ftp-downgrade 209.165.200.224 1238.tar ap1240_102301
```

config ap username

ユーザ名とパスワードを特定のアクセス ポイントまたはすべてのアクセス ポイントにアクセスするように割り当てるには、**config ap username** コマンドを使用します。

config ap username *user_id* **password** *passwd* ［**all** | *ap_name*］

構文の説明

user_id	管理者ユーザ名。
passwd	管理者パスワード。
all	（任意）すべてのアクセス ポイントを指定します。
ap_name	特定のアクセス ポイントの名前。

コマンド デフォルト

なし

次に、特定のアクセス ポイントにユーザ名およびパスワードを割り当てる例を示します。

```
(Cisco Controller) > config ap username jack password blue la204
```

次に、すべてのアクセス ポイントに同じユーザ名とパスワードを割り当てる例を示します。

```
(Cisco Controller) > config ap username jack password blue all
```

config ap venue

アクセス ポイントに対して 802.11u ネットワークの場所の情報を設定するには、**config ap venue** コマンドを使用します。

config ap venue {**add***venue_name venue-group venue-type lang-code cisco-ap* | **delete**}

構文の説明

add	場所の情報を追加します。
venue_name	場所の名前。
venue_group	場所グループのカテゴリ。場所グループ マッピングの詳細については次の表を参照してください。
venue_type	場所のタイプ。この値は指定された場所グループによって異なります。場所グループ マッピングについては次の表を参照してください。
lang_code	使用する言語。言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。言語の最初の 3 文字を英語で入力します（たとえば、英語の場合は eng）。
cisco_ap	アクセス ポイントの名前。
deletes	場所の情報を削除します。

コマンド デフォルト

なし

次に、cisco-ap1 という名前のアクセス ポイントの場所の詳細を設定する例を示します。

```
(Cisco Controller) > config ap venue add test 11 34 eng cisco-ap1
```

この表には、場所グループごとに異なる場所のタイプが示されます。

表 *5:* 場所グループのマッピング

場所グループの名前	値	グループの場所のタイプ
未指定	0	

場所グループの名前	値	グループの場所のタイプ
アセンブリ	1	• 0：未指定のアセンブリ • 1：アリーナ • 2：スタジアム • 3：乗客ターミナル（たとえば、空港、バス、フェリー、電車の駅） • 4：円形劇場 • 5：アミューズメントパーク • 6：礼拝所 • 7：会議場 • 8：図書館 • 9：博物館 • 10：レストラン • 11：シアター • 12：バー • 13：喫茶店 • 14：動物園または水族館 • 15：緊急対応センター
ビジネス	2	• 0：未指定のビジネス • 1：医師または歯科医師のオフィス • 2：銀行 • 3：消防署 • 4：警察署 • 6：郵便局 • 7：専門家のオフィス • 8：研究および開発施設 • 9：弁護士のオフィス

場所グループの名前	値	グループの場所のタイプ
教育機関	3	• 0：未指定の教育機関 • 1：小学校 • 2：中学校 • 3：大学
工場および産業	4	• 0：未指定の工場および産業 • 1：工場
機関	5	• 0：未指定の公共機関 • 1：病院 • 2：長期看護施設（療養所、ホスピスなど） • 3：アルコールおよび薬物のリハビリテーション センター • 4：グループ ホーム • 5：刑務所または拘置所
商業	6	• 0：未指定の商業施設 • 1：小売店 • 2：食料品店 • 3：自動車サービス ステーション • 4：ショッピング モール • 5：ガソリン スタンド
住居	7	• 0：未指定の居住施設 • 1：私邸 • 2：ホテルまたはモーテル • 3：寄宿舎 • 4：宿泊施設

場所グループの名前	値	グループの場所のタイプ
倉庫	8	未指定の倉庫
公共施設、その他	9	0：未指定の公共施設およびその他
乗り物	10	• 0：未指定の乗り物 • 1：自動車またはトラック • 2：飛行機 • 3：バス • 4：フェリー • 5：船またはボート • 6：電車 • 7：モーター バイク
アウトドア	11	• 0：未指定のアウトドア • 1：自治体メッシュ ネットワーク • 2：都市公園 • 3：休憩施設 • 4：交通管制施設 • 5：バス停留所 • 6：売店

config ap wlan

Cisco Lightweight アクセス ポイント無線に対して無線 LAN オーバーライドを有効または無効にするには、**config ap wlan** コマンドを使用します。

config ap wlan {**enable** | **disable**} {**802.11a** | **802.11b**} *wlan_id cisco_ap*

構文の説明

enable	アクセス ポイントで無線 LAN オーバーライドを有効にします。
disable	アクセス ポイントで無線 LAN オーバーライドを無効にします。
802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
wlan_id	無線 LAN に割り当てられている Cisco ワイヤレス LAN コントローラ ID。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、AP03 802.11a で無線 LAN オーバーライドを有効にする例を示します。

```
(Cisco Controller) > config ap wlan 802.11a AP03
```

config atf 802.11

config atf 802.11 コマンドを使用することにより、ネットワーク レベル、AP グループ レベル、または AP 無線レベルで Cisco Air Time Fairness を設定します。

config atf 802.11{**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} {[*ap-group-name*] | [*ap-name*]}} | {**optimization** {**enable** | **disable**}}

構文の説明

a	802.11a ネットワーク設定を指定します。
b	802.11b/g ネットワーク設定を指定します。
mode	Cisco ATF の強制のきめ細かさを設定します。
disable	Cisco ATF を無効にします。
monitor	Cisco ATF をモニタ モードで設定します。
enforce-policy	Cisco ATF を強制モードで設定します。
optimization	通信時間の最適化を設定します。
enable	通信時間の最適化を有効にします。
disable	通信時間の最適化を無効にします。

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

- 802.11a ネットワークで Cisco ATF をモニタ モードで設定するには、次のコマンドを入力します。

```
(Cisco Controller) >config atf 802.11a mode monitor
```

- 802.11a ネットワークで通信時間の最適化を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config atf 802.11a optimization enable
```

config atf policy

Cisco Air Time Fairness（ATF）ポリシーを設定するには、**config atf policy** コマンドを使用します。

config atf policy {{ **create** *policy-id policy-name policy-weight*} | {**modify** { **weight** *policy-weight policy-name*} | {**client-sharing** {**enable** | **disable**} *policy-name*}} | { **delete** *policy-name*}}

構文の説明

create	通信時間ポリシーを作成します。
modify	通信時間ポリシーを変更します。
delete	通信時間ポリシーを削除します。
client-sharing {**enable** | **disable** *policy-name*}	指定したポリシー名の Client Fair Sharing を有効または無効にします。
policy-id	ポリシー ID（1 ～ 511）。
policy-name	Cisco ATF ポリシーの名前。
policy-weight	ポリシー ウェイト（5 ー 100）。

コマンド履歴

リリース	変更内容
8.1.122.0	このコマンドが追加されました。
8.2	**client-sharing** {**enable** | **disable**} オプションが追加されました。

次に、Cisco ATF ポリシーを作成する例を示します。

```
(Cisco Controller) >config atf policy create 2 test-policy 70
```

config auth-list add

認可済みアクセス ポイント エントリを作成するには、**config auth-list add** コマンドを使用します。

config auth-list add {**mic** | **ssc**} *AP_MAC* [*AP_key*]

構文の説明

mic	アクセス ポイントに製造元がインストールした証明書があることを指定します。
ssc	アクセス ポイントに自己署名証明書があることを指定します。
AP_MAC	Cisco Lightweight アクセス ポイントの MAC アドレス。
AP_key	（任意）20 バイトまたは 40 桁に等しいキー ハッシュ値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレス 00:0b:85:02:0d:20 で製造元がインストールした証明書によって許可済みアクセス ポイント エントリを作成する例を示します。

```
(Cisco Controller) > config auth-list add 00:0b:85:02:0d:20
```

関連コマンド

config auth-list delete

config auth-list ap-policy

config auth-list ap-policy

アクセス ポイントの認可ポリシーを設定するには、**config auth-list ap-policy** コマンドを使用します。

config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **ssc** {**enable** | **disable**}}

構文の説明

authorize-ap enable	許可ポリシーを有効にします。
authorize-ap disable	AP 許可ポリシーを無効にします。
ssc enable	自己署名証明書を持つ AP の接続を許可します。
ssc disable	自己署名証明書を持つ AP の接続を禁止します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントの許可ポリシーを有効にする例を示します。

```
(Cisco Controller) > config auth-list ap-policy authorize-ap enable
```

次に、自己署名証明書を持つアクセス ポイントの接続を有効にする例を示します。

```
(Cisco Controller) > config auth-list ap-policy ssc disable
```

関連コマンド

config auth-list delete

config auth-list add

config auth-list delete

アクセス ポイント エントリを削除するには、**config auth-list delete** コマンドを使用します。

config auth-list delete *AP_MAC*

構文の説明

AP_MAC	Cisco Lightweight アクセス ポイントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレス 00:1f:ca:cf:b6:60 のアクセス ポイント エントリを削除する例を示します。

```
(Cisco Controller) > config auth-list delete 00:1f:ca:cf:b6:60
```

関連コマンド

config auth-list delete

config auth-list add

config auth-list ap-policy

config avc profile create

新しい Application Visibility and Control（AVC）プロファイルを作成するには、**config avc profile create** コマンドを使用します。

config avc profile *profile_name* **create**

構文の説明

profile_name	AVC プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。
create	新しい AVC プロファイルを作成します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

コントローラ 1 台に最大 16 の AVC プロファイルを設定し、AVC プロファイル 1 つを複数の WLAN に関連付けることができます。1 つの WLAN には AVC プロファイルを 1 つだけ設定できます。また各 AVC プロファイルに最大 32 のルールを設定できます。各ルールはアプリケーションに対してマーキングまたは廃棄アクションを指定し、WLAN ごとに最大 32 のアプリケーションのアクションを設定できます。

次に、新しいポート プロファイルを作成する例を示します。

```
(Cisco Controller) > config avc profile avcprofile1 create
```

関連コマンド

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug avc error

debug avc events

config avc profile delete

Application Visibility and Control（AVC）プロファイルを削除するには、**config avc profile delete** コマンドを使用します。

config avc profile *profile_name* **delete**

構文の説明

profile_name	AVC プロファイルの名前。
delete	AVC プロファイルを削除します。

コマンド デフォルト

AVC プロファイルは削除されません。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、AVC プロファイルを削除する例を示します。

```
(Cisco Controller) > config avc profile avcprofile1 delete
```

関連コマンド

config avc profile create

config avc profile rule

config wlan avc

show avc profile summary

show avc profile detailed

debug avc error

debug avc events

config avc profile rule

Application Visibility and Control（AVC）プロフィルのルールを設定するには、**config avc profile rule** コマンドを使用します。

config avc profile *profile_name* **rule** {**add** | **remove**} **application** *application_name* {**drop** | **mark** *dscp*}

構文の説明

profile_name	AVC プロファイルの名前。
rule	AVC プロファイルのルールを設定します。
add	AVC プロファイルのルールを作成します。
remove	AVC プロファイルのルールを削除します。
application	ドロップまたはマークする必要のあるアプリケーションを指定します。
application_name	アプリケーションの名前。ライセンス名は最大 32 文字の英数字で、大文字と小文字を区別します。
drop	選択したアプリケーションに対応するアップストリームおよびダウンストリーム パケットをドロップします。
mark	ドロップダウン リストで指定した DiffServ コード ポイント（DSCP）の値を使用して、選択したアプリケーションに対応するアップストリームおよびダウンストリーム パケットをマークします。DSCP 値を使用して、QoS レベルに基づいて Differentiated Services を提供できます。
dscp	インターネット上で QoS を定義するために使用されるパケット ヘッダー コード。範囲は 0 ～ 63 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、AVC プロファイルのルールを設定する例を示します。

```
(Cisco Controller) > config avc profile avcprofile1 rule add application gmail mark 10
```

関連コマンド

config avc profile delete

config avc profile create

config wlan avc

show avc profile

show avc applications

show avc statistics

debug avc error

debug avc events

config band-select cycle-count

帯域幅選択プローブ サイクル カウントを設定するには、**config band-select cycle-count** コマンドを使用します。

config band-select cycle-count *count*

構文の説明

count	1 ～ 10 の間のサイクル カウントの値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、帯域幅選択のプローブ サイクルカウントを 8 に設定する例を示します。

```
(Cisco Controller) > config band-select cycle-count 8
```

関連コマンド

config band-select cycle-threshold

config band-select expire

config band-select client-rssi

config band-select cycle-threshold

新しいスキャン サイクルの時間のしきい値を設定するには、**config band-select cycle-threshold** コマンドを使用します。

config band-select cycle-threshold *threshold*

構文の説明

threshold	1 ～ 1000 ミリ秒のサイクルしきい値の値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、しきい値が 700 ミリ秒の新しいスキャン サイクルの時間のしきい値を設定する例を示します。

```
(Cisco Controller) > config band-select cycle-threshold 700
```

関連コマンド

config band-select cycle-count

config band-select expire

config band-select client-rssi

config band-select expire

帯域幅選択に対してエントリの期限切れを設定するには、**config band-select expire** コマンドを使用します。

config band-select expire {**suppression** | **dual-band**} *seconds*

構文の説明

suppression	抑制の期限切れを帯域幅選択に設定します。
dual-band	デュアル バンドの期限切れを帯域幅選択に設定します。
seconds	• 10 ～ 200 秒の抑制の値。 • 10 ～ 300 秒のデュアル バンドの値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、抑制の期限切れを 70 秒に設定する例を示します。

```
(Cisco Controller) > config band-select expire suppression 70
```

関連コマンド

config band-select cycle-threshold

config band-select client-rssi

config band-select cycle-count

config band-select client-rssi

帯域幅選択に対して、クライアントの Received Signal Strength Indicator（RSSI）のしきい値を設定するには、**config band-select client-rssi** コマンドを使用します。

config band-select client-rssi *rssi*

構文の説明

rssi	20 ～ 90 のプローブに応答するクライアント RSSI の最小 dBM。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、帯域幅選択の RSSI しきい値を 70 に設定する例を示します。

```
(Cisco Controller) > config band-select client-rssi 70
```

関連コマンド

config band-select cycle-threshold

config band-select expire

config band-select cycle-count

config boot

Cisco ワイヤレス LAN コントローラのブート オプションを変更するには、**config boot** コマンドを使用します。

config boot {**primary** | **backup**}

構文の説明

primary	アクティブとしてプライマリ イメージを設定します。
backup	アクティブとしてバックアップ イメージを設定します。

コマンド デフォルト

デフォルトのブート オプションは **primary** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

各 Cisco ワイヤレス LAN コントローラは、プライマリの、最後にロードされたオペレーティング システム イメージ（OS）をブートオフしたり、バックアップの、以前にロードされた OS イメージをブートオフしたりできます。

次に、LAN コントローラがプライマリの、最後にロードされたイメージをブートオフできるように、プライマリ イメージをアクティブとして設定する例を示します。

```
(Cisco Controller) > config boot primary
```

次に、LAN コントローラがバックアップの、以前にロードされた OS イメージをブートオフできるように、バックアップ イメージをアクティブとして設定する例を示します。

```
(Cisco Controller) > config boot backup
```

関連コマンド

show boot

config call-home contact email address

Call Home 連絡先の電子メール アドレスを設定するには、**config call-home contact-email-addr** コマンドを使用します。

config call-home contact-email-addr *email-address*

構文の説明

email-address	Call Home 連絡先の電子メール アドレス。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home 連絡先の電子メール アドレスを追加する例を示します。

```
(Cisco Controller) >config call-home contact-email-addr device1@example1.com
```

config call-home events

Call Homeイベント レポートを有効または無効にするには、**call-home events** コマンドを使用します。

config call-home events {**enable** | **disable**}

構文の説明

enable	Call Homeイベント レポートを有効にします。
disable	Call Homeイベント レポートを無効にします。

コマンド デフォルト

Enable

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home イベント レポートを無効にする例を示します。

```
(Cisco Controller) > config call-home events disable
```

config call-home http-proxy ipaddr

レポートの HTTP プロキシ アドレスを設定するには、**config call-home http-proxy ipaddr** コマンドを使用します。

config call-home http-proxy ipaddr *ip-address* **port** *port*

構文の説明

ip-address	HTTP プロキシ IP アドレス。
port	HTTP プロキシ ポート番号。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、HTTP プロキシ IP アドレスを使用して Call Home を設定する例を示します。

```
(Cisco Controller) >config call-home http-proxy ipaddr 209.165.200.224 port 773
```

config call-home http-proxy ipaddr 0.0.0.0

レポートの HTTP プロキシ設定をリセットするには、**config call-home http-proxy ipaddr 0.0.0.0** コマンドを使用します。

config call-home http-proxy ipaddr *0.0.0.0*

構文の説明

0.0.0.0	HTTP プロキシ設定をリセットします。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home HTTP プロキシ設定をリセットする例を示します。

```
(Cisco Controller) >config call-home http-proxy ipaddr 0.0.0.0
```

config call-home profile

Call Home プロファイルの作成および更新するには、**config call-home profile** コマンドを使用します。

config call-home profile {**create** | **update** } *profile-name* {**sm-license-data** | **all** | **call-home-data**}{**short-text** | **long-text** | **xml** } *url*

構文の説明

create	Call Home プロファイルを作成します
update	Call Home プロファイルを更新します
sm-license-data	スマートライセンス レポート プロファイルを設定します。
all	すべてのモジュールのレポート プロファイルを設定します。
call-home-data	Call Home データ レポート プロファイルを設定します。
short-text	ショートテキスト形式のデータ レポートを設定します。
long-text	ロングテキスト形式のデータ レポートを設定します。
xml	XML 形式のデータ レポートを設定します。
url	URL 名

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、XML 形式の Call Home レポート プロファイルを作成する例を示します。

```
(Cisco Controller) > config call-home profile create example-profile sm-license-data xml
 internal.example.com
```

config call-home profile delete

Call homeプロファイルを削除するには、**config call-home profile delete** コマンドを使用します。

config call-home profile delete *profile-name*

構文の説明		
	profile-name	Call Home プロファイルは削除されます。

コマンド履歴		
	リリース	変更内容
	8.2	このコマンドが導入されました。

次に、Call Home プロファイルを削除する例を示します。

```
(Cisco Controller) > config call-home profile delete example-profile
```

config call-home profile status

ユーザ プロファイルを有効または無効にするには、**config call-home profile status** コマンドを使用します。

config call-home profile status {**enable** | **disable**}

構文の説明

enable	Call Home プロファイルのステータスを有効にします。
disable	Call Home プロファイルのステータスを無効にします。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home プロファイルを無効にする例を示します。

```
(Cisco Controller) >config call-home profile status disable
```

config call-home reporting

データ レポートのプライバシー レベルを設定するには、**config call-home reporting data-privacy level** コマンドを使用します。

config call-home reporting data-privacy level {**normal** | **high**}**hostname** ホスト名

構文の説明

normal	すべての標準レベル コマンドをスクラビング処理します。
high	標準レベル コマンドと IP ドメイン名および IP アドレスのコマンドをスクラビング処理します。
hostname	すべての高レベル コマンドとホスト名のコマンドをスクラビング処理します。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、標準プライバシー レベルを設定する例を示します。

```
(Cisco Controller) >config call-home reporting data-privacy- level normal hostname
internal.example.com
```

config call-home tac-profile

TAC プロファイルを有効または無効にするには、**config call-home tac-profile status** コマンドを使用します。

config call-home tac-profile status {**enable** | **disable**}

構文の説明

enable	Call Home TAC プロファイルを有効にします。
disable	Call Home TAC プロファイルを無効にします。

コマンド デフォルト

Enable

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home TAC プロファイルを無効にする例を示します。

```
(Cisco Controller) >config call-home tac-profile status disable
```

config cdp

コントローラ上に Cisco Discovery Protocol（CDP）を設定するには、**config cdp** コマンドを使用します。

config cdp {**enable** | **disable** | **advertise-v2** {**enable** | **disable**} | **timer***seconds* | **holdtime** *holdtime_interval*}

構文の説明

enable	コントローラで CDP をイネーブルにします。
disable	コントローラで CDP をディセーブルにします。
advertise-v2	CDP バージョン 2 のアドバタイズメントを設定します。
timer	CDP メッセージが生成される間隔を設定します。
seconds	CDP メッセージが生成される間隔。範囲は 5 ～ 254 秒です。
holdtime	生成された CDP パケット内の存続可能時間の値としてアドバタイズされる時間を設定します。
holdtime_interval	最大ホールド タイマー値。範囲は 10 ～ 255 秒です。

コマンド デフォルト

CDP タイマーのデフォルト値は 60 秒です。

CDP 保持時間のデフォルト値は 180 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CDP 最大ホールド タイマーを 150 秒に設定する例を示します。

```
(Cisco Controller) > config cdp timer 150
```

関連コマンド

config ap cdp

show cdp

show ap cdp

config certificate lsc

ローカルで有効な証明書（LSC）を設定するには、**config certificate lsc** コマンドを使用します。

config certificate lsc {**enable** | **disable** | **ca-server** *http://url:port/path* | **ca-cert** {**add** | **delete**} | **subject-params** *country state city orgn dept email* | **other-params** *keysize*} | **ap-provision** {**auth-list** {**add** | **delete**} *ap_mac* | **revert-cert** *retries*}

構文の説明

enable	コントローラ上で LSC 証明書をイネーブルにします。
disable	コントローラ上で LSC 証明書をディセーブルにします。
ca-server	認証局（CA）サーバ設定を指定します。
http://url:port/path	CA サーバのドメイン名または IP アドレス。
ca-cert	CA 証明書データベースの設定を指定します。
add	CA サーバから CA 証明書を取得し、コントローラの証明書データベースに追加します。
delete	コントローラの証明書データベースから CA 証明書を削除します。
subject-params	デバイス証明書の設定を指定します。
country state city orgn dept email	認証局の国、州、市、組織、部門、および電子メール。 （注） Common Name（CN）は、現在の MIC/SSC 形式である *Cxxxx-MacAddr* を使用して、アクセスポイント上で自動的に生成されます。ここで、*xxxx* は製品番号です。
other-params	デバイスの証明書キーのサイズ設定を指定します。
keysize	384 ～ 2048 の値（ビット単位）。デフォルト値は 2048 です。
ap-provision	アクセスポイントプロビジョニング リストの設定を指定します。

auth-list	プロビジョニング リストの許可設定を指定します。
ap_mac	プロビジョニング リストに追加する、またはプロビジョニング リストから削除するアクセス ポイントの MAC アドレス。
revert-cert	デフォルトの証明書に戻る前にアクセス ポイントが LSC を使用してコントローラへの接続を試行する回数。
retries	0 ～ 255 の値。デフォルト値は 3 です。 （注） 再試行回数を 0 に設定した場合、アクセス ポイントが LSC 使用によるコントローラへの join に失敗すると、このアクセス ポイントはデフォルトの証明書を使用したコントローラへの join を試みません。初めて LSC を設定する場合は、ゼロ以外の値を設定することが推奨されます。

コマンド デフォルト

keysize のデフォルト値は 2048 ビットです。*retries* のデフォルト値は 3 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

1 つの CA サーバだけを設定できます。別の CA サーバを設定するには、**config certificate lsc ca-server delete** コマンドを使用して設定済みの CA サーバを削除してから、別の CA サーバを設定します。

アクセス ポイント プロビジョニング リストを設定する場合は、AP プロビジョニングを有効にしたときに（手順8）プロビジョニング リストのアクセス ポイントだけがプロビジョニングされます。アクセス ポイント プロビジョン リストを設定しない場合、コントローラに接続する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。

次に、LSC 機能を有効にする例を示します。

```
(Cisco Controller) >config certificate lsc enable
```

次に、認証局（CA）サーバ設定の LSC 設定をイネーブルにする例を示します。

```
(Cisco Controller) >config certificate lsc ca-server http://10.0.0.1:8080/caserver
```

次に、CA サーバから CA 証明書を取得し、コントローラの証明書データベースにそれを追加する例を示します。

```
(Cisco Controller) >config certificate lsc ca-cert add
```

次に、2048 ビットのキー サイズの LSC 証明書を設定する例を示します。

```
(Cisco Controller) >config certificate lsc keysize 2048
```

config certificate ssc

自己署名証明書（SSC）で証明書を設定するには、**config certificate ssc** コマンドを使用します。

config certificate ssc hash validation {**enable** | **disable**}

構文の説明

hash	SSC のハッシュ キーを設定します。
validation	SSC 証明書のハッシュ検証を設定します。
enable	SSC 証明書のハッシュ検証をイネーブルにします。
disable	SSC証明書のハッシュ検証をディセーブルにします。

コマンド デフォルト

SSC 証明書は、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

SSC ハッシュ検証をイネーブルにすると、AP は仮想コントローラの SSC 証明書を検証します。AP が SSC 証明書を検証するときに、仮想コントローラのハッシュ キーが、フラッシュに保存されるハッシュ キーと一致するかどうかが確認されます。一致が見つかると、検証は成功し、APはRun状態に移行します。一致がない場合、検証は失敗し、APはコントローラから切断され、ディスカバリ プロセスを再起動します。デフォルトでは、ハッシュ検証は有効です。AP は仮想コントローラに関連付ける前に、フラッシュの仮想コントローラのハッシュ キーが必要です。SSC のハッシュ検証をディセーブルにすると、AP はハッシュ検証をバイパスし、Run 状態に直接移動します。

APS は物理コントローラに関連付けることが可能で、ハッシュ キーをダウンロードし、次に仮想コントローラに関連付けます。APが物理コントローラに関連付けられている場合に、ハッシュ検証がディセーブルであると、ハッシュ検証なしで仮想コントローラを接続します。

次に、SSC 証明書のハッシュ検証を有効にする例を示します。

```
(Cisco Controller) > config certificate ssc hash validation enable
```

関連コマンド

show certificate ssc

show mobility group member

config mobility group member hash

config certificate

show certificate compatibility

show certificate lsc

show certificate summary

show local-auth certificates

config certificate use-device-certificate webadmin

Web 管理にデバイス証明書を使用するには、**config certificate use-device-certificate webadmin** コマンドを使用します。

config certificate use-device-certificate webadmin

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web 管理にデバイス証明書を使用する例を示します。

```
(Cisco Controller) > config certificate use-device-certificate webadmin
Use device certificate for web administration. Do you wish to continue? (y/n) y
Using device certificate for web administration.
Save configuration and restart controller to use new certificate.
```

関連コマンド

config certificate

show certificate compatibility

show certificate lsc

show certificate ssc

show certificate summary

show local-auth certificates

config client ccx clear-reports

クライアントのレポート情報をクリアするには、**config client ccx clear-reports** コマンドを使用します。

config client ccx clear-reports *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントの MAC アドレス 00:1f:ca:cf:b6:60 のレポート情報をクリアする例を示します。

```
(Cisco Controller) >config client ccx clear-reports 00:1f:ca:cf:b6:60
```

config client ccx clear-results

コントローラ上のテスト結果をクリアするには、**config client ccx clear-results** コマンドを使用します。

config client ccx clear-results *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントの MAC アドレス 00:1f:ca:cf:b6:60 のテスト結果をクリアする例を示します。

```
(Cisco Controller) >config client ccx clear-results 00:1f:ca:cf:b6:60
```

config client ccx default-gw-ping

デフォルトのゲートウェイ pingテストの実行要求をクライアントに送信するには、**config client ccx default-gw-ping** コマンドを使用します。

config client ccx default-gw-ping *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このテストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアント 00:0b:85:02:0d:20 に要求を送信して、デフォルト ゲートウェイの ping テストを実行する例を示します。

```
(Cisco Controller) >config client ccx default-gw-ping 00:0b:85:02:0d:20
```

config client ccx dhcp-test

DHCP テストの実行要求をクライアントに送信するには、**config client ccx dhcp-test** コマンドを使用します。

config client ccx dhcp-test *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このテストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアント 00:E0:77:31:A3:55 に要求を送信して、DHCP テストを実行する例を示します。

```
(Cisco Controller) >config client ccx dhcp-test 00:E0:77:31:A3:55
```

config client ccx dns-ping

ドメイン ネーム システム（DNS）サーバ IP アドレス ping テストの実行要求をクライアントに送信するには、**config client ccx dns-ping** コマンドを使用します。

config client ccx dns-ping *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このテストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアントに要求を送信して、DNS サーバの IP アドレスの ping テストを実行する例を示します。

```
(Cisco Controller) >config client ccx dns-ping 00:E0:77:31:A3:55
```

config client ccx dns-resolve

指定されたホスト名に対するドメイン ネーム システム（DNS）名前解決テストの実行要求をクライアントに送信するには、**config client ccx dns-resolve** コマンドを使用します。

config client ccx dns-resolve *client_mac_address host_name*

構文の説明

client_mac_address	クライアントの MAC アドレス。
host_name	クライアントのホスト名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このテストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアント 00:E0:77:31:A3:55 に要求を送信して、指定したホスト名に対して DNS 名前解決テストを実行する例を示します。

```
(Cisco Controller) >config client ccx dns-resolve 00:E0:77:31:A3:55 host_name
```

config client ccx get-client-capability

機能情報の送信要求をクライアントに送信するには、**config client ccx get-client-capability** コマンドを使用します。

config client ccx get-client-capability *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアント 172.19.28.40 に機能情報の送信要求を送信する例を示します。

```
(Cisco Controller) >config client ccx get-client-capability 172.19.28.40
```

config client ccx get-manufacturer-info

製造元情報の送信要求をクライアントに送信するには、**config client ccx get-manufacturer-info** コマンドを使用します。

config client ccx get-manufacturer-info *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアント 172.19.28.40 に製造元情報を送信するように要求する例を示します。

```
(Cisco Controller) >config client ccx get-manufacturer-info 172.19.28.40
```

config client ccx get-operating-parameters

現在の動作パラメータの送信要求をクライアントに送信するには、**config client ccx get-operating-parameters** コマンドを使用します。

config client ccx get-operating-parameters *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアント 172.19.28.40 に現在の動作パラメータの送信要求を送信する例を示します。

```
(Cisco Controller) >config client ccx get-operating-parameters 172.19.28.40
```

config client ccx get-profiles

プロファイルの送信要求をクライアントに送信するには、**config client ccx get-profiles** コマンドを使用します。

config client ccx get-profiles *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアント 172.19.28.40 にプロファイルの詳細の送信要求を送信する例を示します。

```
(Cisco Controller) >config client ccx get-profiles 172.19.28.40
```

config client ccx log-request

特定のクライアント デバイスの Cisco Client Extensions（CCX）ログ要求を設定するには、**config client ccx log-request** コマンドを使用します。

config client ccx log-request {**roam** | **rsna** | **syslog**} *client_mac_address*

構文の説明

roam	（任意）クライアント CCX ローミング ログを指定する要求を指定します。
rsna	（任意）クライアント CCX RSNA ログを指定する要求を指定します。
syslog	（任意）クライアント CCX システム ログを指定する要求を指定します。
client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアント CCS システム ログの指定要求を指定する例を示します。

```
(Cisco Controller) >config client ccx log-request syslog 00:40:96:a8:f7:98
Tue Oct 05 13:05:21 2006
SysLog Response LogID=1: Status=Successful
Event Timestamp=121212121212
Client SysLog = 'This is a test syslog 2'
Event Timestamp=121212121212
Client SysLog = 'This is a test syslog 1'
Tue Oct 05 13:04:04 2006
SysLog Request LogID=1
```

次に、クライアント CCX ローミング ログを指定する例を示します。

```
(Cisco Controller) >config client ccx log-request roam 00:40:96:a8:f7:98
Thu Jun 22 11:55:14 2006
Roaming Response LogID=20: Status=Successful
Event Timestamp=121212121212
Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
Transition Time=100(ms)
Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:55:04 2006
Roaming Request LogID=20
Thu Jun 22 11:54:54 2006
Roaming Response LogID=19: Status=Successful
Event Timestamp=121212121212
Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
Transition Time=100(ms)
Transition Reason: Unspecified Transition Result: Success
```

```
Thu Jun 22 11:54:33 2006  Roaming Request LogID=19
```

次に、クライアント CCX RSNA ログを指定する例を示します。

```
(Cisco Controller) >config client ccx log-request rsna 00:40:96:a8:f7:98
Tue Oct 05 11:06:48 2006
RSNA Response LogID=2: Status=Successful
Event Timestamp=242424242424
Target BSSID=00:0b:85:23:26:70
RSNA Version=1
Group Cipher Suite=00-x0f-ac-01
Pairwise Cipher Suite Count = 2
Pairwise Cipher Suite 0 = 00-0f-ac-02
Pairwise Cipher Suite 1 = 00-0f-ac-04
AKM Suite Count = 2
KM Suite 0 = 00-0f-ac-01
KM Suite 1 = 00-0f-ac-02
SN Capability = 0x1
PMKID Count = 2
PMKID 0 = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
PMKID 1 = 0a 0b 0c 0d 0e 0f 17 18 19 20 1a 1b 1c 1d 1e 1f
802.11i Auth Type: EAP_FAST
RSNA Result: Success
```

config client ccx send-message

メッセージをクライアントに送信するには、**config client ccx send-message** コマンドを使用します。

config client ccx send-message *client_mac_address message_id*

構文の説明

client_mac_address	クライアントの MAC アドレス。

message_id

次のいずれかを含むメッセージ タイプ。

- 1：SSID が無効です。
- 2：ネットワーク設定が無効です。
- 3：WLAN の信頼性に不一致があります。
- 4：ユーザの資格情報が間違っています。
- 5：サポートにお問い合わせください。
- 6：問題は解決されました。
- 7：問題は解決されていません。
- 8：もう一度後で作業を行ってください。
- 9：示された問題を修正してください。
- 10：ネットワークにより、トラブルシューティングが拒否されました。
- 11：クライアント レポートを取得中です。
- 12：クライアント ログを取得中です。
- 13：取得が完了しました。
- 14：アソシエーション テストを開始します。
- 15：DHCP テストを開始します。
- 16：ネットワーク接続テストを開始します。
- 17：DNS ping テストを開始します。
- 18：名前解決テストを開始します。
- 19：802.1X 認証テストを開始します。
- 20：クライアントを特定のプロファイルにリダイレクトしています。
- 21：テストが完了しました。
- 22：テストに合格しました。
- 23：テストに失敗しました。
- 24：通常の操作を再開するには、診断チャネル操作をキャンセルするか、WLAN プロファイルを選択してください。

	• 25：クライアントにより、ログの取得が拒否されました。 • 26：クライアントにより、クライアントレポートの取得が拒否されました。 • 27：クライアントにより、テスト要求が拒否されました。 • 28：無効なネットワーク（IP）設定です。 • 29：ネットワークで機能停止または問題が発生しています。 • 30：予定された保守期間です。 （次ページに続く）
message_type（続き）	• 31：WLAN セキュリティ方式が正しくありません。 • 32：WLAN 暗号化方式が正しくありません。 • 33：WLAN 認証方式が正しくありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メッセージ user-action-required を使用して、クライアント MAC アドレス 172.19.28.40 にメッセージを送信する例を示します。

```
(Cisco Controller) >config client ccx send-message 172.19.28.40 user-action-required
```

config client ccx stats-request

統計要求を送信するには、**config client ccx stats-request** コマンドを使用します。

config client ccx stats-request *measurement_duration* {**dot11** | **security**} *client_mac_address*

構文の説明

measurement_duration	秒単位の測定期間。
dot11	（任意）dot11 カウンタを指定します。
security	（任意）セキュリティ カウンタを指定します。
client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、dot11 カウンタの設定を指定する例を示します。

```
(Cisco Controller) >config client ccx stats-request 1 dot11 00:40:96:a8:f7:98
Measurement duration = 1
dot11TransmittedFragmentCount       = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount                    = 3
dot11RetryCount                     = 4
dot11MultipleRetryCount             = 5
dot11FrameDuplicateCount            = 6
dot11RTSSuccessCount                = 7
dot11RTSFailureCount                = 8
dot11ACKFailureCount                = 9
dot11ReceivedFragmentCount          = 10
dot11MulticastReceivedFrameCount    = 11
dot11FCSErrorCount                  = 12
dot11TransmittedFrameCount          = 13
```

config client ccx test-abort

現在のテストの中止要求をクライアントに送信するには、**config client ccx test-abort** コマンドを使用します。

config client ccx test-abort *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

一度に保留できるテストは 1 つだけです。

次に、クライアントに要求を送信して、現在のテストの設定を中止する例を示します。

```
(Cisco Controller) >config client ccx test-abort 11:11:11:11:11:11
```

config client ccx test-association

アソシエーション テストの実行要求をクライアントに送信するには、**config client ccx test-association** コマンドを使用します。

config client ccx test-association *client_mac_address ssid bssid* **802.11**{**a** | **b** | **g**} *channel*

構文の説明

client_mac_address	クライアントの MAC アドレス。
ssid	ネットワーク名。
bssid	Basic SSID。
802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
802.11g	802.11g ネットワークを指定します。
channel	チャネル番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントの MAC アドレス 00:0E:77:31:A3:55 に要求を送信して、基本 SSID アソシエーション テストを実行する例を示します。

```
(Cisco Controller) >config client ccx test-association 00:E0:77:31:A3:55 ssid bssid
802.11a
```

config client ccx test-dot1x

802.1x テストの実行要求をクライアントに送信するには、**config client ccx test-dot1x** コマンドを使用します。

config client ccx test-dot1x *client_mac_address profile_id bssid* **802.11** {**a** | **b** | **g**} *channel*

構文の説明

client_mac_address	クライアントの MAC アドレス。
profile_id	テスト プロファイル名。
bssid	Basic SSID。
802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
802.11g	802.11g ネットワークを指定します。
channel	チャネル番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントに要求を送信して、プロファイル名 profile_01 で 802.11b テストを実行する例を示します。

```
(Cisco Controller) >config client ccx test-dot1x 172.19.28.40 profile_01 bssid 802.11b
```

config client ccx test-profile

プロファイル リダイレクト テストの実行要求をクライアントに送信するには、**config client ccx test-profile** コマンドを使用します。

config client ccx test-profile *client_mac_address profile_id*

構文の説明

client_mac_address	クライアントの MAC アドレス。
profile_id	テスト プロファイル名。 （注） *profile_id* には、必ずクライアント レポートが有効なクライアント プロファイルのプロファイル ID を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントに要求を送信して、プロファイル名 profile_01 でプロファイル リダイレクト テストを実行する例を示します。

```
(Cisco Controller) >config client ccx test-profile 11:11:11:11:11:11 profile_01
```

config client deauthenticate

クライアントを接続解除するには、**config client deauthenticate** コマンドを使用します。

config client deauthenticate {*MAC* | *IPv4/v6_address* | *user_name*}

構文の説明

MAC	Client MAC address.
IPv4/v6_address	IPv4 または IPv6 アドレス。
user_name	クライアント ユーザ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレスを使用してクライアントを認証解除する例を示します。

```
(Cisco Controller) >config client deauthenticate 11:11:11:11:11:11
```

config client location-calibration

リンク集約を設定するには、**config client location-calibration** コマンドを使用します。

config client location-calibration {**enable** *mac_address interval* | **disable** *mac_address*}

構文の説明

enable	（任意）クライアントのロケーション調整をイネーブルにするよう指定します。
mac_address	クライアントの MAC アドレス。
interval	秒単位の測定間隔。
disable	（任意）クライアントのロケーション調整をディセーブルにするよう指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、45 秒の測定間隔で、クライアント 37:15:85:2a のクライアント ロケーション調整を無効にする例を示します。

```
(Cisco Controller) >config client location-calibration enable 37:15:86:2a:Bc:cf 45
```

config client profiling delete

クライアント プロファイルを削除するには、**config client profiling** コマンドを使用します。

config client profiling delete {*mac_address*}

構文の説明

mac_address	クライアントの MAC アドレス。

コマンド履歴

リリース	変更内容
8.2	このコマンドは本リリースで追加されました。

次に、クライアント プロファイルを削除する例を示します。

```
(Cisco Controller) >config client profiling delete 37:15:86:2a:Bc:cf
```

（注） 上記のコマンドを実行すると、デバイス タイプが「Unknown」に変更されます。クライアントは削除されませんが、代わりにクライアントのプロファイル情報が削除され、クライアントは依然として関連付けられているために保持されます。Cisco WLC のアーキテクチャ上の制限により、CLI の確認メッセージは表示されません。

config coredump

クラッシュ後のコントローラによるコア ダンプ ファイルの生成を有効または無効にするには、**config cordump** コマンドを使用します。

config coredump {**enable** | **disable**}

構文の説明

enable	コントローラによるコア ダンプ ファイルの生成をイネーブルにします。
disable	コントローラによるコア ダンプ ファイルの生成をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クラッシュ後のコントローラによるコア ダンプ ファイルの生成を有効にする例を示します。

```
(Cisco Controller) > config coredump enable
```

関連コマンド

config coredump ftp

config coredump username

show coredump summary

config coredump ftp

クラッシュ後に FTP サーバにコントローラのコア ダンプ ファイルを自動的にアップロードするには、**config coredump ftp** コマンドを使用します。

config coredump ftp *server_ip_address filename*

構文の説明

server_ip_address	コントローラがコア ダンプ ファイルを送信する FTP サーバの IP アドレス。
filename	コントローラのコア ダンプ ファイルに割り当てられた名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

使用上のガイドライン

このコマンドを使用するには、コントローラが FTP サーバに到達できる必要があります。

次に、*core_dump_controller* という名前のコア ダンプ ファイルをネットワーク アドレス *192.168.0.13* で FTP サーバにアップロードするようにコントローラを設定する例を示します。

```
(Cisco Controller) > config coredump ftp 192.168.0.13 core_dump_controller
```

関連コマンド

config coredump

config coredump username

show coredump summary

config coredump username

クラッシュ後にコントローラのコア ダンプ ファイルをアップロードするときの FTP サーバのユーザ名とパスワードを指定するには、**config coredump username** コマンドを使用します。

config coredump username *ftp_username* **password** *ftp_password*

構文の説明

ftp_username	FTP サーバ ログイン ユーザ名。
ftp_password	FTP サーバ ログイン パスワード。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用するには、コントローラが FTP サーバに到達できる必要があります。

次に、コア ダンプ ファイル アップロードに対して、FTP サーバにユーザ名 *admin* とパスワード *adminpassword* を指定する例を示します。

```
(Cisco Controller) > config coredump username admin password adminpassword
```

関連コマンド

config coredump ftp

config coredump

show coredump summary

config country

コントローラの国コードを設定するには、**config country** コマンドを使用します。

config country *country_code*

構文の説明

country_code	2 文字または 3 文字の国コード。

コマンド デフォルト

us（米国の国コード）。

使用上のガイドライン

Cisco WLC は、ネットワーク管理者または資格のある IP プロフェッショナルがインストールしてください。その際、正しい国コードを選択する必要があります。インストール後は、法的な規制基準を遵守するためおよび、適切なユニット機能を保証するために、ユニットへのアクセスはパスワードで保護する必要があります。最新の国コードおよび規制区域については、関連する製品マニュアルを参照してください。

サポートされている国のリストを表示するには、**show country** コマンドを使用できます。

次に、コントローラの国コードを DE に設定する例を示します。

```
(Cisco Controller) >config country DE
```

config cts sxp

コントローラで Cisco TrustSec SXP（CTS）接続を設定するには、**config cts sxp** コマンドを使用します。

config cts sxp {**enable** | **disable** | **connection** {**delete** | **peer**} | **default password** *password* | **retry period** *time-in-seconds*}

構文の説明

enable	コントローラで CTS 接続を有効にします。
disable	コントローラで CTS 接続を無効にします。
connection	コントローラで CTS 接続を設定します。
delete	コントローラで CTS 接続を削除します。
peer	コントローラが接続されるネクストホップ スイッチを設定します。
ip-address	ピアの IPv4アドレスのみ。
default password	SXP メッセージの MD5 認証のデフォルト パスワードを設定します。
password	SXP メッセージの MD5 認証用のデフォルト パスワード。パスワードには、少なくとも 6 文字が必要です。
retry period	SXP 再試行期間を設定します。
time-in-seconds	接続の失敗後に CTS の接続を再試行するまでの時間。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

リリース 8.0 では、TrustSec SXP の設定で IPv4 のみがサポートされています。

次に、コントローラで CTS を有効にする例を示します。

```
(Cisco Controller) > config cts sxp enable
```

次に、CTS 接続のピアを設定する例を示します。

```
> config cts sxp connection peer 209.165.200.224
```

関連コマンド

debug cts sxp

config custom-web ext-webauth-mode

カスタム Web 認証ページに対する外部 URL Web ベースのクライアント認可を設定するには、**config custom-web ext-webauth-mode** コマンドを使用します。

config custom-web ext-webauth-mode {**enable** | **disable**}

構文の説明

enable	外部 URL Web ベースのクライアント認証をイネーブルにします。
disable	外部 URL Web ベースのクライアント認証をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、外部 URL Web ベースのクライアント認証を有効にする例を示します。

```
(Cisco Controller) > config custom-web ext-webauth-mode enable
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-url show custom-web

config custom-web ext-webauth-url

カスタム Web 認証ページに対する完全な外部 Web 認証 URL を設定するには、**config custom-web ext-webauth-url** コマンドを使用します。

config custom-web ext-webauth-url *URL*

構文の説明

URL	Web ベースのクライアント認証に使用される URL。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web ベースのクライアント認証に、完全な外部 Web 認証 URL http://www.AuthorizationURL.com/ を設定する例を示します。

```
(Cisco Controller) > config custom-web ext-webauth-url http://www.AuthorizationURL.com/
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode show custom-web

config custom-web ext-webserver

外部 Web サーバを設定するには、**config custom-web ext-webserver** コマンドを使用します。

config custom-web ext-webserver {**add** *index IP_address* | **delete** *index*}

構文の説明

add	外部 Web サーバを追加します。
index	外部 Web サーバ リストの外部 Web サーバ インデックス。インデックスは 1 から 20 までの数にしてください。
IP_address	外部 Web サーバの IP アドレス。
delete	外部 Web サーバを削除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

次に、外部 Web サーバ 2 のインデックスを、外部 Web サーバの IP アドレス 192.23.32.19 に追加する例を示します。

```
(Cisco Controller) > config custom-web ext-webserver add 2 192.23.32.19
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web logout-popup

カスタムWeb認証のログアウトポップアップを有効または無効にするには、**config custom-web logout-popup** コマンドを使用します。

config custom-web logout-popup {**enable** | **disable**}

構文の説明

enable	カスタム Web 認証のログアウト ポップアップをイネーブルにします。このページは、ログインの成功後、またはカスタム Web 認証ページのリダイレクト後に表示されます。
disable	カスタム Web 認証のログアウト ポップアップをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、カスタム Web 認証のログアウト ポップアップを無効にする例を示します。

```
(Cisco Controller) > config custom-web logout-popup disable
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-url show custom-web

config custom-web radiusauth

RADIUS Web 認証方式を設定するには、**config custom-web radiusauth** コマンドを使用します。

config custom-web radiusauth {**chap** | **md5chap** | **pap**}

構文の説明

chap	RADIUS Web 認証方式をチャレンジ ハンドシェイク認証プロトコル（CHAP）に設定します。
md5chap	RADIUS Web 認証方式を Message Digest 5 CHAP（MD5 CHAP）に設定します。
pap	RADIUS Web 認証方式をパスワード認証プロトコル（PAP）に設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS Web 認証方式を MD5-CHAP に設定する例を示します。

```
(Cisco Controller) > config custom-web radiusauth md5chap
```

関連コマンド

config custom-web redirectUrl

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web redirectUrl

カスタム Web 認証ページのリダイレクト URL を設定するには、**config custom-web redirectUrl** コマンドを使用します。

config custom-web redirectUrl *URL*

構文の説明

URL	指定したアドレスにリダイレクトされるURL。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、abc.com にリダイレクトされる URL を設定する例を示します。

```
(Cisco Controller) > config custom-web redirectUrl abc.com
```

関連コマンド

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web sleep-client

Web 認証されたスリープ状態のクライアントを削除するには、**config custom-web sleep-client** コマンドを使用します。

config custom-web sleep-client delete *mac_address*

構文の説明

delete	Web 認証されたスリープ状態のクライアントを、そのクライアントの MAC アドレスの使用して削除します。
mac_address	スリープ状態のクライアントの MAC アドレス。

コマンド デフォルト

Web 認証されたスリープ状態のクライアントは削除されません。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

次に、Web 認証されたスリープ状態のクライアントを削除する例を示します。

```
(Cisco Controller) > config custom-web sleep-client delete 0:18:74:c7:c0:90
```

config custom-web webauth-type

Web 認証のタイプを設定するには、**config custom-web webauth-type** コマンドを使用します。

config custom-web webauth-type {**internal** | **customized** | **external**}

構文の説明

internal	Web 認証タイプを internal に設定します。
customized	Web 認証タイプを customized に設定します。
external	Web 認証タイプを external に設定します。

コマンド デフォルト

デフォルトの Web 認証タイプは **internal** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

Web 認証タイプを internal に設定する例を示します。

```
(Cisco Controller) > config custom-web webauth-type internal
```

関連コマンド

config custom-web redirectUrl

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web weblogo

カスタム Web 認証ページの Web 認証ロゴを設定するには、**config custom-web weblogo** コマンドを使用します。

config custom-web weblogo {**enable** | **disable**}

構文の説明

enable	Web 認証のロゴ設定をイネーブルにします。
disable	Web認証のロゴ設定をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、Web 認証ロゴを有効にする例を示します。

```
(Cisco Controller) > config custom-web weblogo enable
```

関連コマンド

config custom-web redirectUrl

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web webmessage

カスタム Web 認証ページのカスタム Web 認証メッセージを設定するには、**config custom-web webmessage** コマンドを使用します。

config custom-web webmessage *message*

構文の説明

message	Web 認証のメッセージ テキスト。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web 認証のメッセージのテキスト Thisistheplace を設定する例を示します。

```
(Cisco Controller) > config custom-web webmessage Thisistheplace
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web webtitle

カスタム Web 認証ページの Web 認証タイトル テキストを設定するには、**config custom-web webtitle** コマンドを使用します。

config custom-web webtitle *title*

構文の説明

title	Web 認証のカスタム タイトル テキスト。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web 認証のカスタム タイトル テキスト Helpdesk を設定する例を示します。

```
(Cisco Controller) > config custom-web webtitle Helpdesk
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config database size

ローカル データベースを設定するには、**config database size** コマンドを使用します。

config database size *count*

構文の説明

count	512 ～ 2040 のデータベース サイズ値

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

show database コマンドを使用して、ローカル データベースの設定を表示します。

次に、ローカル データベースのサイズを設定する例を示します。

```
(Cisco Controller) > config database size 1024
```

関連コマンド

show database

config dhcp

内部 DHCP を設定するには、**config dhcp** コマンドを使用します。

config dhcp {**address-pool** *scope start end* | **create-scope** *scope* | **default-router** *scope router_1* [*router_2*] [*router_3*] | **delete-scope** *scope* | **disable** *scope* | **dns-servers** *scope dns1* [*dns2*] [*dns3*] | **domain** *scope domain* | **enable** *scope* | **lease** *scope lease_duration* | **netbios-name-server** *scope wins1* [*wins2*] [*wins3*] | **network***scope network netmask*}

config dhcpopt-82 remote-id {*ap_mac* | *ap_mac*:*ssid* | *ap-ethmac* | *apname:ssid* | *ap-group-name* | *flex-group-name* | *ap-location* | *apmac-vlan_id* | *apname-vlan_id* | *ap-ethmac-ssid* }

構文の説明

address-pool *scope start end*	割り当てるアドレス範囲を設定します。スコープ名およびアドレス範囲の最初と最後のアドレスを指定する必要があります。
create-scope *name*	新規 DHCP スコープを作成します。スコープ名を指定する必要があります。
default-router *scope router_1* [*router_2*] [*router_3*]	指定されたスコープのデフォルト ルータを設定し、ルータの IP アドレスを指定します。オプションで、セカンダリおよびターシャリ ルータの IP アドレスを指定できます。
delete-scope *scope*	指定された DHCP スコープを削除します。
disable *scope*	指定された DHCP スコープをディセーブルにします。
dns-servers *scope dns1* [*dns2*] [*dns3*]	指定されたスコープのネーム サーバを設定します。少なくとも 1 つのネーム サーバを指定する必要があります。オプションでセカンダリおよびターシャリ ネーム サーバを指定できます。
domain *scope domain*	DNS ドメイン名を設定します。スコープ名およびドメイン名を指定する必要があります。
enable *scope*	指定された DHCP スコープをイネーブルにします。
lease *scope lease_duration*	指定されたスコープのリース期間（秒）を設定します。

netbios-name-server *scope wins1* [*wins2*] [*wins3*]	NetBIOS ネーム サーバを設定します。スコープ名およびネームサーバのIPアドレスを指定する必要があります。オプションで、セカンダリおよびターシャリ ネーム サーバの IP アドレスを指定できます。
network *scope network netmask*	network および netmask を設定します。スコープ名、ネットワーク アドレス、およびネットワーク マスクを指定する必要があります。
opt-82 remote-id	DHCP オプション 82 リモート ID フィールド フォーマットを設定します。 DHCP オプション 82 では、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティが強化されます。コントローラは DHCP リレー エージェントとして機能し、信頼できないソースからの DHCP クライアント要求を回避します。コントローラは、要求を DHCP サーバに転送する前に、クライアントからの DHCP 要求にオプション 82 情報を追加します。
ap_mac	DHCP オプション 82 ペイロードへのアクセス ポイントの MAC アドレス。
*ap_mac***:***ssid*	DHCP オプション 82 ペイロードへのアクセス ポイントの MAC アドレスと SSID。
ap-ethmac	AP Ethernet MAC アドレスとしてのリモート ID 形式。
apname:ssid	AP 名としてのリモート ID の形式: SSID。
ap-group-name	AP グループ名としてのリモート ID 形式。
flex-group-name	FlexConnect グループ名としてのリモート ID 形式。
ap-location	AP ロケーションとしてのリモート ID 形式。
apmac-vlan_id	AP 無線の MAC アドレスとしてのリモート ID の形式: VLAN_ID。
apname-vlan_id	AP 名としてのリモート ID の形式: VLAN_ID。
ap-ethmac-ssid	AP Ethernet MAC としてのリモート ID の形式: SSID のアドレス。

コマンド デフォルト

ap-group-name のデフォルト値は「default-group」であり、ap-location のデフォルト値は「default location」です。

ap-group-name と flex-group-name がヌルの場合は、システム MAC がリモート ID フィールドとして送信されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

show dhcp コマンドを使用して、内部 DHCP 設定を表示します。

次に、スコープ 003 の DHCP リースを設定する例を示します。

```
(Cisco Controller) >config dhcp lease 003
```

config dhcp opt-82 format

DHCPオプション 82 の形式を設定するには、**config dhcp opt-82 format** を使用します。

config dhcp opt-82 format{*binary* | *ascii*}

構文の説明

binary	DHCP オプション 82 の形式をバイナリとして指定します。
ascii	DHCP オプション 82 の形式を ASCII として指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、DHCP オプション 82 ペイロードの形式を設定する例を示します。

```
(Cisco Controller) > config dhcp opt-82 format binary
```

config dhcp opt-82 remote-id

DHCPオプション 82 ペイロードの形式を設定するには、**config dhcp opt-82 remote-id** を使用します。

config dhcp opt-82 remote-id {*ap_mac* | *ap_mac:ssid* | *ap-ethmac* | *apname:ssid* | *ap-group-name* | *flex-group-name* | *ap-location* | *apmac-vlan-id* | *apname-vlan-id* | *ap-ethmac-ssid*}

構文の説明

ap_mac	アクセス ポイントの無線 MAC アドレスを DHCP オプション 82 ペイロードに対して指定します。
ap_mac:ssid	アクセス ポイントの無線 MAC アドレスと SSID を DHCP オプション 82 ペイロードに対して指定します。
ap-ethmac	アクセス ポイントのイーサネット MAC アドレスを DHCP オプション 82 ペイロードに対して指定します。
apname:ssid	アクセス ポイントの AP 名と SSID を DHCP オプション 82 ペイロードに対して指定します。
ap-group-name	AP グループ名を DHCP オプション 82 ペイロードに対して指定します。
flex-group-name	FlexConnect グループ名を DHCP オプション 82 ペイロードに対して指定します。
ap-location	AP の場所を DHCP オプション 82 ペイロードに対して指定します。
apmac-vlan-id	アクセス ポイントの無線 MAC アドレスと VLAN ID を DHCP オプション 82 ペイロードに対して指定します。
apname-vlan-id	AP 名とその VLAN ID を DHCP オプション 82 ペイロードに対して指定します。
ap-ethmac-ssid	アクセス ポイントのイーサネット MAC アドレスと SSID を DHCP オプション 82 ペイロードに対して指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、DHCP オプション 82 ペイロードのリモート ID を設定する例を示します。

```
(Cisco Controller) > config dhcp opt-82 remote-id apgroup1
```

config dhcp proxy

DHCP パケットを変更するレベルを指定するには、**config dhcp proxy** コマンドを使用します。

config dhcp proxy {**enable** | **disable** {**bootp-broadcast** [**enable** | **disable**]}

構文の説明

enable	コントローラは制限なしで DHCP パケットを変更できます。
disable	DHCP パケット変更をリレー レベルまで削減します。
bootp-broadcast	DHCP BootP ブロードキャスト オプションを設定します。

コマンド デフォルト

DHCP は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

show dhcp proxy コマンドを使用して、DHCP プロキシ処理のステータスを表示します。

サードパーティ WGB サポートを有効にするには、**config wlan passive-client enable** コマンドを入力して、ワイヤレス LAN 上でパッシブ クライアント機能を有効にする必要があります。

次に、DHCP パケット情報を無効にする例を示します。

```
(Cisco Controller) >config dhcp proxy disable
```

次に、DHCP BootP ブロードキャスト オプションを有効にする例を示します。

```
(Cisco Controller) >config dhcp proxy disable bootp-broadcast enable
```

config dhcp timeout

DHCP タイムアウト値を設定するには、**config dhcp timeout** コマンドを使用します。WLAN が DHCP required 状態に設定されている場合は、このタイマーが、クライアントが DHCP 経由で DHCP リースを取得するまで WLC が待機する時間を制御します。

config dhcp timeout *timeout-value*

構文の説明

timeout-value	5～120 秒の範囲のタイムアウト値。

コマンド デフォルト

デフォルトのタイムアウト値は 120 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、DHCP のタイムアウトを 10 秒に設定する例を示します。

```
(Cisco Controller) >config dhcp timeout 10
```

config exclusionlist

除外リスト エントリを作成または削除するには、**config exclusionlist** コマンドを使用します。

config exclusionlist {**add** *MAC* [*description*] | **delete** *MAC* | **description** *MAC* [*description*]}

構文の説明

config exclusionlist	除外リストを設定します。
add	ローカル除外リスト エントリを作成します。
delete	ローカル除外リスト エントリを削除します。
description	除外リスト エントリの説明を指定します。
MAC	ローカル除外リスト エントリの MAC アドレス。
description	（任意）除外されたエントリの説明（最大 32 文字）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレス *xx:xx:xx:xx:xx:xx* のローカル除外リスト エントリを作成する例を示します。

```
(Cisco Controller) > config exclusionlist add xx:xx:xx:xx:xx:xx lab
```

次に、MAC アドレス *xx:xx:xx:xx:xx:xx* のローカル除外リスト エントリを削除する例を示します。

```
(Cisco Controller) > config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

関連コマンド

show exclusionlist

config flexconnect [ipv6] acl

FlexConnect アクセス ポイントに設定されたアクセス コントロール リストを適用するには、**config flexconnect** [**ipv6**] **acl** コマンドを使用します。IPv6 の FlexConnect ACL を設定するには、**ipv6** キーワードを使用します。

config flexconnect［**ipv6**］ **acl** ｛**apply** ｜ **create** ｜ **delete**｝ *acl_name*

構文の説明

ipv6	IPv6 の FlexConnect ACL を設定するには、このオプションを使用します。このオプションを使用しない場合は、IPv4 の FlexConnect ACL が設定されます。
apply	ACL をデータ パスに適用します。
create	ACL を作成します。
delete	ACL を削除します。
acl_name	最大 32 文字の英数字による ACL 名。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.8	IPv6 ACL オプションが追加されました。

次に、FlexConnect アクセス ポイントに設定された IPv4 の ACL を適用する例を示します。

```
(Cisco Controller) >config flexconnect acl apply acl1
```

config flexconnect [ipv6] acl rule

FlexConnect アクセス ポイントにアクセス コントロール リスト（ACL）ルールを設定するには、**config flexconnect** [**ipv6**] **acl rule** コマンドを使用します。

config flexconnect ［**ipv6**］ **acl rule** ｛**action** *rule_name rule_index* ｛**permit** ｜ **deny**｝ ｜ **add** *rule_name rule_index* ｜ **change index** *rule_name old_index new_index* ｜ **delete** *rule_name rule_index* ｜ **destination address** *rule_name rule_index ip_address netmask* ｜ **destination port range** *rule_name rule_index start_port end_port* ｜ **direction** *rule_name rule_index* ｛**in** ｜ **out** ｜ **any**｝ ｜ **dscp** *rule_name rule_index dscp* ｜ **protocol** *rule_name rule_index protocol* ｜ **source address** *rule_name rule_index ip_address netmask* ｜ **source port range** *rule_name rule_index start_port end_port* ｜ **swap index** *rule_name index_1 index_2*｝

構文の説明

ipv6	IPv6 の FlexConnect ACL ルールを設定するには、このオプションを使用します。このオプションを使用しない場合は、IPv4 の FlexConnect ACL ルールが設定されます。
action	アクセスを許可するか拒否するかを設定します。
rule_name	最大 32 文字の英数字による ACL 名。
rule_index	1 ～ 32 のルールのインデックス。
permit	ルールのアクションを許可します。
deny	ルールのアクションを拒否します。
add	新規ルールを追加します。
change	ルールのインデックスを変更します。
index	ルールのインデックスを指定します。
delete	ルールを削除します。
destination address	ルールの宛先 IP アドレスとネットマスクを設定します。
ip_address	ルールの IP アドレス。
netmask	ルールのネットマスク。
start_port	開始ポート番号（0 ～ 65535）。
end_port	終了ポート番号（0 ～ 65535）。

direction	ルールの方向（in、out、またはany）を設定します。
in	ルールの方向を in に設定します。
out	ルールの方向を out に設定します。
any	ルールの方向を any に設定します。
dscp	ルールの DSCP を設定します。
dscp	0 ～ 63 の数値または **any**。
protocol	ルールの DSCP を設定します。
protocol	0 ～ 255 の数値または **any**。
source address	ルールの送信元 IP アドレスとネットマスクを設定します。
source port range	ルールの送信元ポート範囲を設定します。
swap	ルールの2つのインデックスを入れ替えます。
index_1	交換する最初のインデックス。
index_2	最初のインデックスと交換するルールインデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.8	IPv6 ACL オプションが追加されました。

次に、アクセスを許可するよう ACL を設定する例を示します。

```
(Cisco Controller) >config flexconnect acl rule action lab1 4 permit
```

config flexconnect [ipv6] acl url-domain

FlexConnect ACL の URL ドメイン ベース ルールを設定するには、**config flexconnect acl** [**ipv6**] **url-domain** コマンドを使用します。

config flexconnect ［**ipv6]acl url-domain**{**action** *acl-name index action* |**add** *acl-name index*|**delete** *acl-name index*|**url** *acl-name index url-name*}

構文の説明

ipv6	IPv6 の FlexConnect ACL の URL ドメイン ベース ルールを設定するには、このオプションを使用します。このオプションを使用しない場合は、IPv4 の FlexConnect ACL ルールが設定されます。
action *acl-name index action*	FlexConnect ACL ルールのアクション（アクセスの許可または拒否）を設定します。
add *acl-name index*	FlexConnect ACL に URL ドメインに追加します。
delete *acl-name index*	FlexConnect ACL から URL ドメインを削除します。
url *acl-name index url-name*	FlexConnect ACL の URL 名を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.8	IPv6 ACL オプションが追加されました。

次に、IPv6 の FlexConnect ACL の URL ベース ルールを設定する例を示します。

```
(Cisco Controller) >config flexconnect ipv6 acl url-domain action acls-to-allow 2 permit
```

config flexconnect arp-caching

FlexConnect AP でローカルに切り替えられる WLAN を使用している場合にクライアントの ARP エントリをキャッシュに保存するには、**config flexconnect arp-caching** コマンドを使用します。

config flexconnect arp-caching {**enable** } **disable**}

構文の説明

arp-caching enable	クライアントの ARP エントリをキャッシュに保存し、ローカルに切り替えられる WLAN のクライアントに代わって応答するようにアクセス ポイントに指示します。
arp-caching disable	ARP キャッシュを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、FlexConnect AP でローカルに切り替えられる WLAN を使用している場合にプロキシ ARP を適用する例を示します。

```
(Cisco Controller) >config flexconnect arp-caching enable
```

config flexconnect avc profile

FlexConnect の Application Visibility and Control（AVC）プロファイルのルールを設定するには、**config flexconnect avc profile** コマンドを使用します。

config flexconnect avc profile *profilename* {**create | delete**} | **apply** | **rule** {**addapplication** *app-name* {**drop** | {**mark** *dscp-value*}}} | {**remove application** *app-name*}

構文の説明

proflie-name	AVC プロファイルの名前。入力できる範囲は英数字で 0 ～ 32 文字です。
create	AVC プロファイルを作成します。
delete	AVC プロファイルを削除します。
apply	AVC プロファイルを適用します。
rule	AVC プロファイルのルールを設定します。
add application	AVC プロファイルのルールを追加します。
app-name	アプリケーションの名前。入力できる範囲は英数字で 0 ～ 32 文字です。
drop	パケットをドロップするルールを追加します。
mark	特定の DiffServ コード ポイント（DSCP）によってパケットをマークするルールを追加します。
dscp-value	パケット マーキングの DSCP 値。範囲は 0 ～ 63 です。
remove application	AVC プロファイルのルールを削除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、FlexConnect プロファイルを作成する例を示します。

```
(Cisco Controller) >config flexconnect avc profile profile1 create
```

config flexconnect fallback-radio-shut

イーサネット リンクが動作していないときのアクセス ポイントの無線インターフェイスを設定するには、**config flexconnect fallback-radio-shut** コマンドを使用します。

config flexconnect fallback-radio-shut {**disable** | **enable delay** *delay-in-sec*}

構文の説明

disable	無線インターフェイスのシャットダウンを無効にします。
enable	無線インターフェイスのシャットダウンを有効にします。
delay	インターフェイスの遅延（この後に無線インターフェイスがシャットダウンされる）を指定します。
delay-in-sec	遅延時間（秒単位）。

コマンド デフォルト

無線インターフェイスのシャットダウンは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。

使用上のガイドライン

無線インターフェイスのシャットダウンを有効にする場合のみ、遅延時間を指定できます。

次に、5 秒間の遅延時間後の無線インターフェイス シャットダウンを有効にする例を示します。

```
(Cisco Controller) >config flexconnect fallback-radio-shut enable delay 5
```

config flexconnect group

FlexConnect グループを追加、削除、または設定するには、**config flexconnect group** コマンドを使用します。

config flexconnect group *group_name* {**add** | **delete** | **ap** {**add** | **delete**} *ap-mac* | **radius** {**ap** {**authority** {**id** *hex_id* | **info** *auth_info*} | **disable** | **eap-fast** {**enable** | **disable**} | **enable** | **leap** {**enable** | **disable**} | **pac-timeout** *timeout* | **server-key** {**auto** | *key*} | **user** {**add** {*username password*} | **delete** *username*}}} | **server auth** {**add** | **delete**} {**primary** | **secondary**} *IP_address auth_port secret*} | **predownload** {**disable** | **enable**} | **master** *ap_name* | **slave** {**retry-count** *max_count* | **ap-name** *cisco_ap*} | **start** {**primary backup abort**} | **local-split** {**wlan** *wlan_id* **acl** *acl_name* {**enable** | **disable**}} | **multicast overridden-interface** {**enable** | **disable**} | **vlan** {**add** *vlan_id* **acl** *in-aclname out-aclname* | **delete** *vlan_id* } | **web-auth wlan** *wlan_id* **acl** *acl_name* {**enable** | **disable**} | **web-policy acl** {**add** | **delete**} *acl_name*}

config flexconnect group *group_name* **radius ap** {**eap-cert download** | **eap-tls** {**enable** | **disable**} | **peap** {**enable** | **disable**}}

config flexconnect group *group_name* **policy acl** {**add** | **delete**} *acl_name*

構文の説明

group_name	グループ名。
add	FlexConnect グループを追加します。
delete	FlexConnect グループを削除します。
ap	FlexConnect グループにアクセス ポイントを追加または削除します。
add	FlexConnect グループにアクセス ポイントを追加します。
delete	FlexConnect グループからアクセス ポイントを削除します。
ap_mac	アクセス ポイントの MAC アドレス。
radius	FlexConnect グループのクライアント認証用に RADIUS サーバを設定します。
ap	FlexConnect グループのクライアント認証用にアクセス ポイント ベースの RADIUS サーバを設定します。
authority	拡張認証プロトコル - セキュア トンネル経由の柔軟な認証（EAP-FAST）権限パラメータを設定します。

id	ローカル EAP-FAST サーバの権限識別子を設定します。
hex_id	16 進数文字で表したローカル EAP-FAST サーバの権限識別子。最大 32 文字の 16 進数の偶数を入力できます。
info	テキスト形式のローカル EAP-FAST サーバの権限識別子を設定します。
auth_info	テキスト形式のローカル EAP-FAST サーバの権限識別子。
disable	APベースのRADIUSサーバを無効にします。
eap-fast	拡張認証プロトコル - セキュアトンネル経由の柔軟な認証（EAP-FAST）権限を有効または無効にします。
enable	EAP-FAST 認証を有効にします。
disable	EAP-FAST 認証を無効にします。
enable	APベースのRADIUSサーバを有効にします。
leap	Lightweight Extensible Authentication Protocol（LEAP）認証を有効または無効にします。
disable	LEAP 認証を無効にします。
enable	LEAP 認証をイネーブルにします。
pac-timeout	EAP-FAST Protected Access Credential（PAC）タイムアウト パラメータを設定します。
timeout	PAC タイムアウト（日数単位）。範囲は 2 ～ 4095 です。値 0 は無効であることを示します。
server-key	EAP-FAST サーバ キーを設定します。サーバ キーは、PAC の暗号化と暗号化解除に使用されます。
auto	ランダム サーバ キーを自動的に生成します。
key	FlexConnect グループの効率的なアップグレードを無効にするキー。
user	AP ベースの RADIUS サーバでユーザ リストを管理します。

add	ユーザを追加します。最大 100 人のユーザを設定できます。
username	大文字と小文字を区別し、英数字で最大24 文字のユーザ名。
password	ユーザのパスワード
delete	ユーザを削除します。
server	外部 RADIUS サーバを設定します。
add	外部 RADIUS サーバを追加します。
delete	外部 RADIUS サーバを削除します。
primary	外部プライマリ RADIUSサーバを設定します。
secondary	外部セカンダリ RADIUSサーバを設定します。
IP_address	RADIUS サーバの IP アドレスです。
auth_port	RADIUS サーバのポート アドレスです。
secret	RADIUS サーバのインデックス。
predownload	FlexConnect グループの効率的な AP アップグレードを設定します。アクセス ポイントをリセットしたり、ネットワーク接続を切断したりせずに、コントローラからアクセス ポイントにアップグレード イメージをダウンロードできます。
disable	FlexConnect グループの効率的なアップグレードを無効にします。
enable	FlexConnect グループの効率的なアップグレードを有効にします。
master	マスター AP として FlexConnect グループのアクセス ポイントを手動で指定します。
ap_name	アクセス ポイント名。
slave	スレーブ AP として FlexConnect グループのアクセス ポイントを手動で指定します。
retry-count	スレーブ アクセス ポイントがマスターからイメージをプレダウンロードを試みる回数を設定します。

max_count	スレーブ アクセス ポイントがマスターからイメージをプレダウンロードを試みる最大回数。
ap_name	手動で設定したマスターをオーバーライドします。
cisco_ap	マスター アクセス ポイントの名前。
start	FlexConnect グループのプレダウンロード イメージ アップグレードを開始します。
primary	FlexConnect グループのプレダウンロードのプライマリ・イメージのアップグレードを開始します。
backup	FlexConnect グループのプレダウンロードのバックアップ イメージのアップグレードを開始します。
abort	FlexConnect グループのプレダウンロード イメージ アップグレードを中断します。
local-split	WLAN 単位で、FlexConnect AP グループにローカル スプリット ACL を設定します。
wlan	FlexConnect AP グループにローカル・スプリット ACL の WLAN を設定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
acl	WLAN 単位で、FlexConnect AP グループにローカル スプリット ACL を設定します。
acl_name	ACL の名前
multicast overridden-interface	ローカルにスイッチされたクライアントの上書きインターフェイスで、レイヤ 2 ブロードキャスト ドメイン間のマルチキャストを設定します。
vlan	FlexConnect グループに VLAN を設定します。
add	FlexConnect グループに VLAN を追加します。
vlan_id	VLAN 識別番号。
in-acl	最大 32 文字の英数字による着信 ACL 名。
out-acl	最大 32 文字の英数字による発信 ACL 名。

delete	FlexConnect グループから VLAN を削除。
web-auth	外部 Web 認証の FlexConnect ACL を設定します。
wlan	FlexConnect ACL を設定する無線 LAN を指定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	FlexConnect アクセス ポイントの名前。
acl	FlexConnect ACL を設定します。
web-policy	Web ポリシー FlexConnect ACL を設定します。
add	FlexConnect グループに Web ポリシー FlexConnect ACL を追加します。
delete	FlexConnect グループから Web ポリシー FlexConnect ACL を削除します
eap-cert download	EAP ルートおよびデバイス証明書をダウンロードします。
eap-tls	EAP-Transport Layer Security（EAP-TLS）認証を有効または無効にします。
peap	Protected Extensible Authentication Protocol（PEAP）認証を有効または無効にします。
policy acl	FlexConnect グループのポリシー ACL を設定します。
http-proxy ipaddress	HTTP プロキシ サーバを設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

最大 100 個のクライアントを追加できます。

リリース 7.4 以降では、RADIUS サーバでサポートされている最大数は 100 です。

次に、MAC アドレス 192.12.1.2 に対して FlexConnect グループを追加する例を示します。

```
(Cisco Controller) >config flexconnect group 192.12.1.2 add
```

次に、サーバのインデックス番号が 1 である FlexConnect グループのプライマリ サーバとして RADIUS サーバを追加する例を示します。

```
(Cisco Controller) >config flexconnect group 192.12.1.2 radius server add primary 1
```

次に、WLAN の FlexConnect AP グループにローカル スプリット ACL を有効にする例を示します。

```
(Cisco Controller) >config flexconnect group flexgroup1 local-split wlan 1 acl flexacl1
 enable
```

config flexconnect group vlan

FlexConnect グループの VLAN を設定するには、**config flexconnect group vlan** コマンドを使用します。

config flexconnect group *group_name* **vlan** {**add** *vlan-id* **acl** *in-aclname out-aclname* | **delete** *vlan-id*}

構文の説明

group_name	FlexConnect グループ名。
add	FlexConnect グループの VLAN を追加します。
vlan-id	VLAN ID。
acl	アクセス コントロール リストを指定します。
in-aclname	インバウンド ACL の名前。
out-aclname	アウトバウンド ACL の名前。
delete	FlexConnect グループから VLAN を削除。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect グループ myflexacl の VLAN ID 1 を追加する例を示します。この例では、インバウンド ACL の名前は in-acl、アウトバウンド ACL の名前は out-acl です。

```
(Cisco Controller) >config flexconnect group vlan myflexacl vlan add 1 acl in-acl out-acl
```

configflexconnectgroup*group-name*dhcpoverridden-interface

FlexConnect グループの DHCP 優先インターフェイスを有効または無効にするには、**config flexconnect group** *group-name* **dhcp overridden-interface** コマンドを使用します。

config flexconnect group *group-name* **dhcp overridden-interface** {**enable** | **disable**}

構文の説明

overridden-interface	FlexConnect グループの DHCP 優先インターフェイス。
group-name	FlexConnect グループの名前。
enable	ローカルで切り替えられるクライアントの DHCP ブロードキャストを有効にするようにアクセス ポイントに指示します。
disable	機能を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、ローカルに切り替えられるクライアントの DHCP ブロードキャストを有効にする例を示します。

```
(Cisco Controller) >config flexconnect
  group flexgroup dhcp overridden-interface enable
```

config flexconnect group web-auth

FlexConnect グループの Web-Auth ACL を設定するには、**config flexconnect group web-auth** コマンドを使用します。

config flexconnect group *group_name* **web-auth wlan** *wlan-id* **acl** *acl-name* {**enable** | **disable**}

構文の説明

group_name	FlexConnect グループ名。
wlan-id	WLAN ID。
acl-name	ACL 名です。
enable	FlexConnect グループの Web-Auth ACL を有効にします。
disable	FlexConnect グループの Web-Auth ACL を無効にします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 1 で、FlexConnect グループ myflexacl の Web-Auth ACL webauthacl を有効にする例を示します。

```
(Cisco Controller) >config flexconnect group myflexacl web-auth wlan 1 acl webauthacl
enable
```

config flexconnect group web-policy

FlexConnect グループの Web ポリシー ACL を設定するには、**config flexconnect group web-policy** コマンドを使用します。

config flexconnect group *group_name* **web-policy acl** {**add** | **delete**} *acl-name*

構文の説明

group_name	FlexConnect グループ名。
add	Web ポリシー ACL を追加します。
delete	Web ポリシー ACL を削除します。
acl-name	Web ポリシー ACL の名前。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect グループ myflexacl に Web ポリシー ACL mywebpolicyacl を追加する例を示します。

```
(Cisco Controller) >config flexconnect group myflexacl web-policy acl add mywebpolicyacl
```

config flexconnect join min-latency

接続時に最短の遅延のコントローラを選択するようアクセス ポイントを有効または無効にするには、**config flexconnect join min-latency** コマンドを使用します。

config flexconnect join min-latency {**enable** | **disable**} *cisco_ap*

構文の説明

enable	接続時に最短の遅延のコントローラを選択するようアクセス ポイントを有効にします。
disable	接続時に最短の遅延のコントローラを選択するようアクセス ポイントを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイント。

コマンド デフォルト

アクセス ポイントは、接続時に最短の遅延のコントローラを選択できません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この機能を有効にすると、アクセスポイントは検出要求と検出応答の間の時間を計算し、最初に応答したコントローラに join します。

この設定は、コントローラの HA 設定よりも優先され、OEAP アクセスポイントにのみ適用されます。

次に、接続時に遅延の最も少ないコントローラをアクセス ポイントが選択できるようにする例を示します。

```
(Cisco Controller) >config flexconnect join min-latency enable CISCO_AP
```

config flexconnect office-extend

OfficeExtend アクセス ポイントの FlexConnect モードを設定するには、**config flexconnect office-extend** コマンドを使用します。

config flexconnect office-extend {{**enable** | **disable**} *cisco_ap* | **clear-personalssid-config** *cisco_ap*}

構文の説明

enable	アクセス ポイントに対して OfficeExtend モードを有効にします。
disable	アクセス ポイントに対して OfficeExtend モードを無効にします。
clear-personalssid-config	アクセス ポイントのパーソナル SSID だけをクリアします。
cisco_ap	Cisco Lightweight アクセス ポイント。

コマンド デフォルト

アクセス ポイントで FlexConnect モードを有効にした場合は、OfficeExtend モードが自動的に有効になります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

現時点では、WPLUS ライセンスにより Cisco 5500 シリーズのコントローラに接続された Cisco Aironet 1130 シリーズおよび 1140 シリーズのアクセス ポイントだけを OfficeExtend アクセス ポイントとして設定できます。

アクセス ポイントに対して OfficeExtend モードを有効にした場合は、不正なアクセス ポイントの検出が自動的に無効になります。多くの場合、室内環境に導入された OfficeExtend アクセス ポイントは、大量の不正なデバイスを検出します。**config rogue detection** コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの不正検出を有効または無効にできます。

アクセス ポイントに対して OfficeExtend モードを有効にした場合は、DTLS データ暗号化が自動的に有効になります。ただし、**config ap link-encryption** コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効または無効にできます。

アクセス ポイントに対して OfficeExtend モードを有効にした場合は、Telnet および SSH アクセスが自動的に無効になります。ただし、**config ap telnet** または **config ap ssh** コマンドを使用して、特定のアクセス ポイントの Telnet または SSH アクセスを有効または無効にできます。

アクセスポイントに対して OfficeExtend モードを有効にした場合は、リンク遅延が自動的に有効になります。ただし、**config ap link-latency** コマンドを使用して、コントローラに現在関連

付けられている特定のアクセス ポイントまたはすべてのアクセス ポイントのリンク遅延を有効または無効にできます。

次に、アクセス ポイント Cisco_ap の office-extend を有効にする例を示します。

```
(Cisco Controller) >config flexconnect office-extend enable Cisco_ap
```

次に、アクセス ポイント Cisco_ap のアクセス ポイントのパーソナル SSID だけをクリアする例を示します。

```
(Cisco Controller) >config flexconnect office-extend clear-personalssid-config Cisco_ap
```

config flow

NetFlow モニタおよびエクスポータを設定するには、**config flow** コマンドを使用します。

config flow {**add** | **delete**} **monitor** *monitor_name* {**exporter** *exporter_name* | **record**{*ipv4_client_app_flow_record* | *ipv4_client_src_dst_flow_record*}

構文の説明

add	エクスポータにNetFlowモニタを関連付けるか、NetFlowモニタにNetFlow レコードを関連付けます。
delete	エクスポータからNetFlowモニタの関連付けを解除するか、NetFlowモニタから NetFlow レコードの関連付けを解除します。
monitor	NetFlow モニタを設定します。
monitor_name	NetFlow モニタの名前。モニタ名は最大 32 文字の英数字で、大文字と小文字を区別します。モニタ名にスペースを含めることはできません。
exporter	NetFlow エクスポータを設定します。
exporter_name	NetFlowエクスポータの名前。モニタ名は最大32文字の英数字で、大文字と小文字が区別されます。エクスポータ名にスペースを含めることはできません。
record	NetFlow モニタに NetFlow レコードを関連付けます。
ipv4_client_app_flow_record	パフォーマンスを向上させる既存のレコード テンプレート。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

エクスポータは、IP トラフィック情報のテンプレートをエクスポートするネットワーク エンティティです。Cisco WLC は、エクスポータとして機能します。Cisco WLC の NetFlow レコードには、クライアントのMACアドレス、クライアントの送信元IPアドレス、WLAN ID、データの入力および出力バイト、入力および出力パケット、入力および出力DiffServ コードポイント（DSCP）など、指定されたフローのトラフィックに関する情報が含まれています。

次に、NetFlow モニタおよびエクスポータを設定する例を示します。

```
(Cisco Controller) > config flow add monitor monitor1 exporter exporter1
```

config guest-lan

無線 LAN を作成したり、削除したり、有効または無効にしたりするには、**config guest-lan** コマンドを使用します。

config guest-lan {**create** | **delete**} *guest_lan_id interface_name* | {**enable** | **disable**} *guest_lan_id*

構文の説明

create	有線 LAN の設定を作成します。
delete	有線 LAN の設定を削除します。
guest_lan_id	1～5 の LAN 識別子。
interface_name	最大 32 文字の英数字のインターフェイス名。
enable	ワイヤレス LAN をイネーブルにします。
disable	ワイヤレス LAN をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LAN ID 16 の無線 LAN を有効にする例を示します。

```
(Cisco Controller) > config guest-lan enable 16
```

関連コマンド

show wlan

config guest-lan custom-web ext-webauth-url

Web ログイン ページにアクセスする前にゲスト ユーザを外部サーバにリダイレクトするには、**config guest-lan custom-web ext-webauth-url** コマンドを使用します。

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

構文の説明

ext_web_url	外部サーバの URL。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LAN ID 16 の無線 LAN を有効にする例を示します。

```
(Cisco Controller) > config guest-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 1
```

関連コマンド

config guest-lan

config guest-lan create

config guest-lan custom-web login_page

config guest-lan custom-web global disable

グローバル カスタム Web 設定ではなくゲスト LAN 固有のカスタム Web 設定を使用するには、**config guest-lan custom-web global disable** コマンドを入力します。

config guest-lan custom-web global disable *guest_lan_id*

構文の説明

guest_lan_id	1 ～ 5 のゲスト LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config guest-lan custom-web global enable *guest_lan_id* コマンドを入力すると、カスタム Web 認証の設定がグローバル レベルで使用されます。

次に、ゲスト LAN ID 1 のグローバル Web 設定を無効にする例を示します。

```
(Cisco Controller) > config guest-lan custom-web global disable 1
```

関連コマンド

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan custom-web login_page

config guest-lan custom-web webauth-type

config guest-lan custom-web login_page

カスタマイズされた Web ログイン ページに有線ゲスト ユーザがログインできるようにするには、**config guest-lan custom-web login_page** コマンドを使用します。

config guest-lan custom-web login_page *page_name guest_lan_id*

構文の説明

page_name	カスタマイズされた Web ログイン ページの名前。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ゲスト LAN ID 1 の Web ログイン ページ custompage1 をカスタマイズする例を示します。

```
(Cisco Controller) > config guest-lan custom-web login_page custompage1 1
```

関連コマンド

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan custom-web webauth-type

有線ゲスト ユーザの Web ログイン ページを定義するには、**config guest-lan custom-web webauth-type** コマンドを使用します。

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

構文の説明

internal	コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
customized	以前に設定されたカスタム Web ログイン ページを表示します。
external	以前に設定された URL へユーザをリダイレクトします。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子。

コマンド デフォルト

コントローラの Web ログイン ページのデフォルト設定は internal です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ゲスト LAN ID 1 の内部として WebAuth タイプでゲスト LAN を設定する例を示します。

```
(Cisco Controller) > config guest-lan custom-web webauth-type internal 1
```

関連コマンド

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan ingress-interface

レイヤ 2 アクセス スイッチ経由で有線ゲスト クライアントとコントローラの間のパスを提供する、有線ゲスト VLAN の入力インターフェイスを設定するには、**config guest-lan ingress-interface** コマンドを入力します。

config guest-lan ingress-interface *guest_lan_id interface_name*

構文の説明

guest_lan_id	1 ～ 5 のゲスト LAN 識別子（両端の値を含む）。
interface_name	インターフェイス名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ゲスト LAN ID 1 およびインターフェイス名 guest01 を使用して有線ゲスト クライアントとコントローラの間にパスを提供する例を示します。

```
(Cisco Controller) > config guest-lan ingress-interface 1 guest01
```

関連コマンド

config interface guest-lan

config guest-lan create

config guest-lan interface

コントローラから有線ゲスト トラフィックを送信する出力インターフェイスを設定するには、**config guest-lan interface** コマンドを入力します。

config guest-lan interface *guest_lan_id interface_name*

構文の説明

guest_lan_id	1 ～ 5 のゲスト LAN 識別子。
interface_name	インターフェイス名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ゲスト LAN ID 1 およびインターフェイス名 guest01 のコントローラからゲスト トラフィックを送信する出力インターフェイスを設定する例を示します。

```
(Cisco Controller) > config guest-lan interface 1 guest01
```

関連コマンド

config ingress-interface guest-lan

config guest-lan create

config guest-lan mobility anchor

モビリティ アンカーを追加または削除するには、**config guest-lan mobility anchor** コマンドを使用します。

config guest-lan mobility anchor {**add** | **delete**} *Guest LAN Id IP addr*

構文の説明

add	WLANにモビリティ アンカーを追加します。
delete	WLAN からモビリティ アンカーを削除します。
Guest LAN Id	1 ～ 5 のゲスト LAN 識別子。
ip-addr	WLAN をアンカーするメンバースイッチの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、WAN ID 4 のモビリティ アンカーおよびアンカー IP *192.168.0.14* を削除する例を示します。

```
(Cisco Controller) > config guest-lan mobility anchor delete 4 192.168.0.14
```

config guest-lan nac

ゲストLANのネットワークアドミッションコントロール（NAC）のアウトオブバンドサポートを有効または無効にするには、**config guest-lan nac** コマンドを使用します。

config guest-lan nac {**enable** | **disable**} *guest_lan_id*

構文の説明

enable	NACアウトオブバンドのサポートをイネーブルにします。
disable	NACアウトオブバンドのサポートをディセーブルにします。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ゲスト LAN ID 3 の NAC アウトオブバンド サポートを有効にする例を示します。

```
(Cisco Controller) > config guest-lan nac enable 3
```

関連コマンド

show nac statistics

show nac summary

config wlan nac

debug nac

config guest-lan security

有線ゲスト LAN のセキュリティ ポリシーを設定するには、**config guest-lan security** コマンドを使用します。

config guest-lan security {**web-auth** {**enable** | **disable** | **acl** | **server-precedence**} *guest_lan_id* | **web-passthrough** {**acl** | **email-input** | **disable** | **enable**} *guest_lan_id*}

構文の説明

web-auth	Web 認証を指定します。
enable	Web 認証の設定をイネーブルにします。
disable	Web 認証の設定をディセーブルにします。
acl	アクセス コントロール リストを設定します。
server-precedence	Web 認証ユーザに対する認証サーバの優先順位を設定します。
guest_lan_id	1～5 の LAN 識別子。
web-passthrough	認証不要の Web キャプティブ ポータルを設定します。
email-input	電子メール アドレスを使用して Web キャプティブ ポータルを設定します。

コマンド デフォルト

有線ゲスト LAN のデフォルトのセキュリティ ポリシーは Web 認証です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ゲスト LAN ID 1 のセキュリティ Web 認証ポリシーを設定する例を示します。

```
(Cisco Controller) > config guest-lan security web-auth enable 1
```

関連コマンド

config ingress-interface guest-lan

config guest-lan create

config interface guest-lan

config interface 3g-vlan

3G/4G-VLAN インターフェイスを設定するには、**config interface 3g-vlan** コマンドを使用します。

config interface 3g-vlan *interface-name* {**enable** | **disable**}

構文の説明

interface-name **enable**	指定された 3G/4G-VLAN インターフェイスを有効にします。
interface-name **disable**	指定された 3G/4G-VLAN インターフェイスを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、3G/4G-VLAN トンネル インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface 3g-vlan vlan-int enable
```

config interface acl

インターフェイスのアクセス コントロール リストを設定するには、**config interface acl** コマンドを使用します。

config interface acl {**ap-manager** | **management** | *interface_name*} {*ACL* | **none**}

構文の説明

ap-manager	アクセス ポイントのマネージャ インターフェイスを設定します。
management	管理インターフェイスを設定します。
interface_name	インターフェイス名。
ACL	最大 32 文字の英数字の ACL 名。
none	何も指定しません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、アクセス コントロール リストを [None] の値で設定する例を示します。

```
(Cisco Controller) > config interface acl management none
```

config interface address

インターフェイスのアドレス情報を設定するには、**config interface address** コマンドを使用します。

config interface address {**ap-manager** *IP_address netmask gateway* | **management** *IP_address netmask gateway* | **service-port** *IP_address netmask* | **virtual** *IP_address* | **dynamic-interface** *IP_address dynamic_interface netmask gateway* | **redundancy-management** *IP_address* **peer-redundancy-management** *IP_address* }

構文の説明

ap-manager	アクセス ポイントのマネージャ インターフェイスを指定します。
IP_address	IP アドレス（IPv4 のみ）。
netmask	ネットワーク マスク。
gateway	ゲートウェイの IP アドレス。
management	管理インターフェイスを指定します。
service-port	アウトオブバンド サービス ポート インターフェイスを指定します。
virtual	バーチャル ゲートウェイ インターフェイスを指定します。
interface-name	*interface-name* パラメータでインターフェイスを指定します。
interface-name	インターフェイス名。
redundancy-management	冗長管理インターフェイスの IP アドレスを設定します。
peer-redundancy-management	ピア冗長管理インターフェイスの IP アドレスを設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

管理インターフェイスは、デフォルトで AP マネージャ インターフェイスとして動作します。

このコマンドは、IPv4 アドレスだけに適用されます。

両方のコントローラの管理インターフェイスが同じサブネット上にあることを確認します。両方のコントローラの冗長管理の IP アドレスが同じであるようにします。同様に、両方のコントローラのピア冗長管理の IP アドレスが同じであるようにします。

次に、IP アドレス 209.165.201.31、ネットワーク マスク 255.255.0.0、およびゲートウェイ アドレス 209.165.201.30 によってアクセス ポイントのマネージャ インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface address ap-manager 209.165.201.31 255.255.0.0
209.165.201.30
```

次に、コントローラの冗長管理インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface address redundancy-management 209.4.120.5
peer-redundancy-management 209.4.120.6
```

次に、仮想インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface address virtual 192.0.2.1
```

関連コマンド

show interface

config interface address redundancy-management

コントローラの管理インターフェイス IP アドレス、サブネット、およびゲートウェイを設定するには、**config interface address redundancy-management** コマンドを使用します。

config interface address redundancy-management *IP_address netmask gateway*

構文の説明

IP_address	アクティブ コントローラの管理インターフェイス IP アドレス。
netmask	ネットワーク マスク。
gateway	ゲートウェイの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、キープアライブが失敗したときのアクティブ/スタンバイの到達可能性を確認できます。。

次に、コントローラの管理 IP アドレスを設定する例を示します。

```
(Cisco Controller) > config interface address redundancy-management 209.165.201.31
255.255.0.0 209.165.201.30
```

関連コマンド

config redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy peer-route

config redundancy unit

config redundancy timer

show redundancy timers

show redundancy summary

debug rmgr

debug rsyncmgr

config interface ap-manager

管理または動的インターフェイスでアクセス ポイントのマネージャ機能を有効または無効にするには、**config interface ap-manager** コマンドを使用します。

config interface ap-manager {**management** | *interface_name*} {**enable** | **disable**}

構文の説明

management	管理インターフェイスを指定します。
interface_name	動的インターフェイス名。
enable	動的インターフェイスでアクセス ポイントのマネージャ機能をイネーブルにします。
disable	動的インターフェイスでアクセス ポイントのマネージャ機能をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

管理インターフェイスに対して動的 AP 管理を有効または無効にするには **management** オプションを使用します。Cisco 5500 シリーズ コントローラの場合、管理インターフェイスはデフォルトで AP マネージャ インターフェイスのように動作します。必要に応じて、管理インターフェイスをAPマネージャ インターフェイスとして無効にし、別の動的インターフェイスを AP マネージャとして作成できます。

動的インターフェイスに対してこの機能を有効にした場合、動的インターフェイスは AP マネージャ インターフェイスとして設定されます（1 つの物理ポートに対して 1 つの AP マネージャ インターフェイスだけが許可されます）。APマネージャ インターフェイスとして指定された動的インターフェイスは WLAN インターフェイスとして使用できません。

次に、アクセス ポイントのマネージャ myinterface を無効にする例を示します。

```
(Cisco Controller) > config interface ap-manager myinterface disable
```

config interface create

有線ゲスト ユーザ アカウントのダイナミック インターフェイス（VLAN）を作成するには、**config interface create** コマンドを使用します。

config interface create *interface_name vlan-id*

構文の説明

interface_name	インターフェイス名。
vlan-id	VLAN 識別番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、lab2 および VLAN ID 6 という名前のインターフェイスによってダイナミック インターフェイスを作成する例を示します。

```
(Cisco Controller) > config interface create lab2 6
```

config interface delete

ダイナミック インターフェイスを削除するには、**config interface delete** コマンドを使用します。

config interface delete *interface-name*

構文の説明

interface-name	*interface-name*インターフェイス名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、VLAN501 という名前のダイナミック インターフェイスを削除する例を示します。

```
(Cisco Controller) > config interface delete VLAN501
```

config interface dhcp management

管理インターフェイスで DHCP オプションを設定するには、**config interface dhcp management** コマンドを使用します。

config interface dhcp management {**option-82** {**bridge-mode-insertion** {**enable** | **disable**} | **enable** | **disable** | **linksel** {**enable** | **disable** | **relaysrc** *interface-name*} | **vpnsel** {**enable** | **disable** | **vpnid** *vpn-id* | **vrfname** *vrf-name*}} | **primary** *primary-dhcp_server* [**secondary** *secondary-dhcp_server*] | **proxy-mode** {**enable** | **disable** | **global**} }

構文の説明

option-82	インターフェイスで DHCP オプション 82 を設定します。
bridge-mode-insertion	DHCP オプション 82 挿入をブリッジモードで設定します。
disable	機能を無効にします。
enable	機能を有効にします。
linksel	ダイナミック インターフェイスまたは管理インターフェイスでリンク選択サブオプション 5 を設定します。
relaysrc	リレー送信元でリンク選択サブオプション 5 を設定します。
interface-name	DHCP サーバから到達可能な既存の WLC インターフェイスの名前。
vpnid	VPN 選択サブオプション 151 VPN ID を設定します。
vpn-id	oui:vpn-index 形式 xxxxxx:xxxxxxxx の VPN ID。
vrfname	VPN 選択サブオプション 151 VPF 名を設定します。
vrf-name	VRF 名（長さ 7 の文字列）。
primary	プライマリ DHCP サーバを指定します。
primary-dhcp-server	サーバの IP アドレス。
secondary	（任意）セカンダリ DHCP サーバを指定します。
secondary-dhcp-server	サーバの IP アドレス。

proxy-mode	インターフェイスで DHCP プロキシ モードを設定します。
global	インターフェイスでグローバル DHCP プロキシ モードを使用します。
disable	（任意）インターフェイスで DHCP プロキシ モードをディセーブルにします。
global	（任意）インターフェイスでグローバル DHCP プロキシ モードを使用します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	新しいキーワード **linksel** と **vpnsel** が追加されました。 このコマンドは、このリリースから IPv6 をサポートしています。

使用上のガイドライン

IPv6 の場合は DHCP プロキシがサポートされず、無効モードで機能します。

次に、管理インターフェイスでオプション 82 を設定する例を示します。

```
(Cisco Controller) > config interface dhcp management option-82 enable
```

関連コマンド

config dhcp
config dhcp proxy
config interface dhcp
config wlan dhcp_server
debug dhcp
debug dhcp service-port
debug disable-all
show dhcp
show dhcp proxy
show interface

config interface dhcp

config interface dhcp コマンドを入力して、管理インターフェイスまたはダイナミック インターフェイスでブリッジ モードの DHCP オプション 82 挿入を設定します。

config interface dhcp {**management** | **dynamic-interface** *dynamic-interface-name*} **option-82 bridge-mode-insertion** {**enable** | **disable**}

構文の説明

management	管理インターフェイス
dynamic-interface	ダイナミック インターフェイス
dynamic-interface-name	ダイナミック インターフェイス名。
option-82	インターフェイスの DHCP オプション 82
bridge-mode-insertion	ブリッジ モード挿入を設定する場合。

コマンド デフォルト

ブリッジ モードの DHCP オプション 82 挿入は無効になっています。

コマンド履歴

リリース	変更内容
8.0	このリリースで、ブリッジモード挿入パラメータが導入されました。

config interface address

インターフェイス アドレスを設定するには、**config interface address** コマンドを使用します。

config interface address {**dynamic-interface** *dynamic_interface netmask gateway* | **management** | **redundancy-management** *IP_address* **peer-redundancy-management** | **service-port** *netmask* | **virtual**} *IP_address*

構文の説明

dynamic-interface	コントローラの動的インターフェイスを設定します。
dynamic_interface	コントローラの動的インターフェイス。
IP_address	インターフェイスの IP アドレス。
netmask	インターフェイスのネットマスク。
gateway	インターフェイスのゲートウェイ。
management	管理インターフェイスの IP アドレスを設定します。
redundancy-management	冗長管理インターフェイスの IP アドレスを設定します。
peer-redundancy-management	ピア冗長管理インターフェイスの IP アドレスを設定します。
service-port	アウトバンドサービス ポートを設定します。
virtual	仮想ゲートウェイ インターフェイスを設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

両方のコントローラの管理インターフェイスが同じサブネット上にあることを確認します。両方のコントローラの冗長管理 IP アドレスが同じであることと、両方のコントローラのピア冗長管理 IP アドレスが同じであることを確認します。

次に、コントローラの冗長管理インターフェイスを設定する例を示します。

```
(Cisco Controller) >config interface address redundancy-management 209.4.120.5
peer-redundancy-management 209.4.120.6
```

次に、仮想インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface address virtual 1.1.1.1
```

関連コマンド

show interface group summary

show interface summary

config interface guest-lan

ゲスト LAN VLAN を有効または無効にするには、**config interface guest-lan** コマンドを使用します。

config interface guest-lan *interface_name* {*enable* | *disable*}

構文の説明

interface_name	インターフェイス名。
enable	ゲスト LAN をイネーブルにします。
disable	ゲスト LAN をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、myinterface という名前のインターフェイスでゲスト LAN 機能を有効にする例を示します。

```
(Cisco Controller) > config interface guest-lan myinterface enable
```

関連コマンド

config guest-lan create

config interface hostname

仮想ゲートウェイ インターフェイスのドメイン ネーム システム（DNS）ホスト名を設定するには、**config interface hostname** コマンドを使用します。

config interface hostname virtual *DNS_host*

構文の説明

virtual	完全記述DNS名の指定された仮想アドレスを使用する仮想ゲートウェイ インターフェイスを指定します 仮想ゲートウェイ IP アドレスは、任意の架空で未割り当ての IP アドレス（192.0.2.1 など）であり、レイヤ 3 Security Manager と Mobility Manager で使用されます。
DNS_host	DNS ホスト名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、完全修飾 DNS ホスト名 DNS_Host の指定された仮想アドレスを使用する仮想ゲートウェイ インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface hostname virtual DNS_Host
```

config interface nasid

インターフェイスのネットワーク アクセス サーバの ID（NAS-ID）を設定するには、**config interface nasid** コマンドを使用します。

config interface nasid {*NAS-ID* | **none**} *interface_name*

構文の説明

NAS-ID	インターフェイスのネットワーク アクセス サーバの ID（NAS-ID）。NAS-ID は、認証要求を使用してコントローラによって（RADIUS クライアントとして）RADIUS サーバに送られます。これはユーザをさまざまなグループに分類するために使用されます。最大 32 文字の英数字を入力できます。 NAS-ID をインターフェイス、WLAN、またはアクセス ポイント グループに設定できます。優先順位は AP グループの NAS-ID > WLAN の NAS-ID > インターフェイスの NAS-ID の順です。
none	コントローラのシステム名を NAS-ID として設定します。
interface_name	最大 32 文字の英数字のインターフェイス名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

AP グループ、WLAN、またはインターフェイスのコントローラに設定されている NAS-ID が認証に使用されます。NAS-ID はコントローラに伝播されません。

次に、インターフェイスの NAS-ID を設定する例を示します。

```
(Cisco Controller) > config interface nasid
```

関連コマンド

config wlan nasid

config wlan apgroup

config interface nat-address

1 対 1 マッピング ネットワーク アドレス変換（NAT）を使用しているルータまたは他のゲートウェイ デバイスの背後に Cisco 5500 シリーズ コントローラを設置するには、**config interface nat-address** コマンドを使用します。

config interface nat-address {**management** | **dynamic-interface** *interface_name*} {{**enable** | **disable**} | {**set** *public_IP_address*}}

構文の説明

management	管理インターフェイスを指定します。
dynamic-interface *interface_name*	動的インターフェイス名を指定します。
enable	インターフェイスで 1 対 1 マッピング NAT をイネーブルにします。
disable	インターフェイスで 1 対 1 マッピング NAT をディセーブルにします。
public_IP_address	外部 NAT IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

これらの NAT コマンドは、Cisco 5500 シリーズ コントローラ専用であり、管理インターフェイスが動的 AP 管理用に設定されている場合にだけ使用できます。

これらのコマンドは、1 対 1 マッピング NAT での使用に対してだけサポートされています。各プライベート クライアントはグローバル アドレスに対して直接的かつ固定的にマッピングされます。クライアントのグループを単一の IP アドレスで表すために送信元ポート マッピングを使用する 1 対多 NAT はサポートされません。

次に、管理インターフェイスで 1 対 1 マッピング NAT を有効にする例を示します。

```
(Cisco Controller) > config interface nat-address management enable
```

次に、管理インターフェイスで外部 NAP IP アドレス 10.10.10.10 を設定する例を示します。

```
(Cisco Controller) > config interface nat-address management set 10.10.10.10
```

config interface port

インターフェイスに物理ポートをマップするには（リンク集約トランクが設定されていない場合）、**config interface port** コマンドを使用します。

config interface port {**management** | *interface_name* | **redundancy-management**} *primary_port* [*secondary_port*]

構文の説明

management	管理インターフェイスを指定します。
interface_name	インターフェイス名。
redundancy-management	冗長性管理インターフェイスを指定します。
primary_port	プライマリ物理ポート番号。
secondary_port	（任意）セカンダリ物理ポート番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

Cisco 5500 シリーズ コントローラ以外のすべてのコントローラに対して **management** オプションを使用できます。

次に、LAb02 インターフェイスのプライマリ ポート番号を 3 に設定する例を示します。

```
(Cisco Controller) > config interface port lab02 3
```

config interface quarantine vlan

いずれかの動的インターフェイスで検疫 VLAN を設定するには、**config interface quarantine vlan** コマンドを使用します。

config interface quarantine vlan *interface-name vlan_id*

構文の説明

interface-name	インターフェイスの名前。
vlan_id	VLAN 識別番号。 （注） 隔離処理を無効にするには、0 と入力します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、VLAN ID 10 がある隔離インターフェイスで隔離 VLAN を設定する例を示します。

```
(Cisco Controller) > config interface quarantine vlan quarantine 10
```

config interface vlan

インターフェイスの VLAN ID を設定するには、**config interface vlan** コマンドを使用します。

config interface vlan {**ap-manager** | **management** | *interface-name* | **redundancy-management**} *vlan*

構文の説明

ap-manager	アクセス ポイントのマネージャ インターフェイスを設定します。
management	管理インターフェイスを設定します。
interface_name	インターフェイス名。
vlan	VLAN 識別番号。
redundancy-management	冗長性管理インターフェイスを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

システム冗長性管理インターフェイスが冗長性ポートにマッピングされている場合は、冗長性管理 VLAN を変更できません。まず冗長性管理ポートを設定する必要があります。

次に、管理インターフェイスの VLAN ID 10 を設定する例を示します。

```
(Cisco Controller) > config interface vlan management 10
```

config interface group mdns-profile

インターフェイス グループに mDNS（マルチキャスト DNS）プロファイルを設定するには、**config interface group mdns-profile** コマンドを使用します。

config interface group mdns-profile {**all** | *interface-group-name*} {*profile-name* | **none**}

構文の説明

all	すべてのインターフェイス グループに mDNS プロファイルを設定します。
interface-group-name	mDNS プロファイルが関連付けられる必要のあるインターフェイス グループの名前。インターフェイス グループ名では大文字と小文字が区別され、最大 32 文字のの英数字を使用できます。
profile-name	mDNS プロファイルの名前。
none	インターフェイス グループから既存の mDNS プロファイルを削除します。インターフェイス グループに mDNS プロファイルを設定することはできません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

mDNS プロファイルが WLAN に関連付けられている場合は、エラーが表示されます。

次に、インターフェイス グループ floor1 に mDNS プロファイルを設定する例を示します。

```
(Cisco Controller) > config interface group mdns-profile floor1 profile1
```

関連コマンド

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config mdns profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config interface mdns-profile

インターフェイスに mDNS（マルチキャスト DNS）プロファイルを設定するには、**config interface mdns-profile** コマンドを使用します。

config interface mdns-profile {**management** | **all** インターフェイス名} {プロファイル名 | **none**}

構文の説明

management	管理インターフェイスの mDNS プロファイルを設定します。
all	すべてのインターフェイスの mDNS プロファイルを設定します。
interface-name	mDNS プロファイルを設定しなければならないインターフェイスの名前。インターフェイス名は最大 32 文字の英数字で、大文字と小文字を区別します。
profile-name	mDNS プロファイルの名前。
none	インターフェイスから既存の mDNS プロファイルを削除します。インターフェイスに mDNS プロファイルを設定することはできません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

mDNS プロファイルが WLAN に関連付けられている場合は、エラーが表示されます。

次に、インターフェイス lab 1 に mDNS プロファイルを設定する例を示します。

```
(Cisco Controller) > config interface mdns-profile lab1 profile1
```

関連コマンド

config mdns query interval

config mdns service

config mdns snooping

config mdns profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config icons delete

フラッシュからアイコンを削除するには、WLAN コンフィギュレーション モードで **config icons delete** コマンドを使用します。

config icons delete { *filename* | **all** }

構文の説明

filename	削除するアイコンの名前。
all	システムからすべてのアイコン ファイルを削除します。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、フラッシュからアイコンを削除する例を示します。

```
Cisco Controller > config icons delete image-1
```

config icons file-info

アイコン パラメータを設定するには、WLAN コンフィギュレーション モードで **config icons file-info** コマンドを使用します。

config icons file-info *filename file-type lang-code width height*

構文の説明

filename	アイコンのファイル名。最大 32 文字を使用できます。
file-type	アイコンのファイル名のタイプまたは拡張子。最大 32 文字を使用できます。
lang-code	アイコンの言語コード。ISO-639 の 2 文字または 3 文字のコードを入力します（たとえば、英語の場合は *eng*）。
width	アイコンの幅。有効な範囲は 1 ～ 65535 です。
height	アイコンの高さ。有効な範囲は 1 ～ 65535 です。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、アイコン パラメータを設定する例を示します。

```
Cisco Controller > config icons file-info ima png eng 300 200
```

config ipv6 disable

Cisco WLC で IPv6 をグローバルに無効にするには、**config ipv6 disable** コマンドを使用します。

config ipv6 disable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用すると、コントローラは、すべての IPv6 パケットを廃棄し、クライアントは IPv6 アドレスを受信しません。

次に、コントローラで IPv6 を無効にする例を示します。

```
(Cisco Controller) >config ipv6 disable
```

config ipv6 enable

Cisco WLC で IPv6 をグローバルに有効にするには、**config ipv6 enable** コマンドを使用します。

config ipv6 enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco WLC で IPv6 を有効にする例を示します。

```
(Cisco Controller) >config ipv6 enable
```

config ipv6 acl

Cisco ワイヤレス LAN コントローラで IPv6 ACL を作成または削除し、ACL をデータ パスに適用し、IPv6 ACL のルールを設定するには、**config ipv6 acl** コマンドを使用します。

config ipv6 acl [**apply** | **cpu** | **create** | **delete** | **rule**]
config ipv6 acl apply *name*
config ipv6 acl cpu {*name* | **none**}
config ipv6 acl create *name*
config ipv6 acl delete *name*
config ipv6 acl rule [**action** | **add** | **change** | **delete** | **destination** | **direction** | **dscp** | **protocol** | **source** | **swap**]
config ipv6 acl rule action *name index* {**permit** | **deny**}
config ipv6 acl rule add *name index*
config ipv6 acl rule change index *name old_index new_index*
config ipv6 acl rule delete *name index*
config ipv6 acl rule destination {**address** *name index ip_address prefix-len* | **port range** *name index* }
`config ipv6 acl rule direction` ***name index*** `{in | out | any}`
config ipv6 acl rule dscp *name dscp*
config ipv6 acl rule protocol *name index protocol*
config ipv6 acl rule source {**address** *name index ip_address prefix-len* | **port range** *name index start_port end_port*}
config ipv6 acl rule swap index *name index_1index_2*

構文の説明

apply *name*	IPv6 ACL を適用します。IPv6 ACL 名には最大 32 文字の英数字で使用できます。
cpu *name*	IPv6 ACL を CPU に適用します。
cpu none	IPV6 ACL を使用しない場合は、none を設定します。
create	IPv6 ACL を作成します。
delete	IPv6 ACL を削除します。
rule（**action**）（*name*）（*index*）	IPv6 ACL のルール（アクセスの許可または拒否）を設定します。IPv6 ACL 名には最大 32 文字の英数字を使用でき、IPv6 ACL ルール インデックスには 1 ー 32 を指定できます。
{**permit** | **deny**}	IPv6 ルールのアクションを許可または拒否します。
add *name index*	新しいルールおよびルール インデックスを追加します。
change *name old_index new_index*	ルールのインデックスを変更します。
delete *name index*	ルールおよびルール インデックスを削除します。

destination address *name index ip_addr prefix-len*	ルールの宛先 IP アドレスとプレフィックス長（0 ー 128）を設定します。
destination port *name index*	ルールの宛先ポート範囲を設定します。IPv6 ACL 名を入力し、その ACL のルール インデックスを設定します。
direction *name index* {**in** | **out** | **any**}	ルールの方向（in、out、または any）を設定します。
dscp *name index dscp*	ルールの DSCP を設定します。DSCP のルールインデックスの場合は、0 ー 63 の数字または **any** を選択してください。
protocol *name index protocol*	ルールのプロトコルを設定します。名前を入力し、次のインデックスを設定します：0 ー 255 または **any**
source address *name index ip_address prefix-len*	ルールの送信元 IP アドレスとネットマスクを設定します。
source port range *name index start_port end_port*	ルールの送信元ポート範囲を設定します。
swap index *name index_1 index_2*	ルールの 2 つのインデックスを入れ替えます。

コマンド デフォルト

ACL を追加すると、**config ipv6 acl cpu** はデフォルトで **enabled** に設定されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。。
8.0	このコマンドが更新され、 **cpu** および **none** キーワードと *ipv6_acl_name* 変数が追加されました。

使用上のガイドライン

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、アクセスを許可するよう IPv6 ACL を設定する例を示します。

```
(Cisco Controller) >config ipv6 acl rule action lab1 4 permit
```

次に、インターフェイス ACL を設定する例を示します。

```
(Cisco Controller) > config ipv6 interface acl management IPv6-Acl
```

関連コマンド

show ipv6 acl detailed

show ipv6 acl cpu

config ipv6 capwap

Cisco ワイヤレス LAN コントローラで CAPWAP AP の IPv6 の CAPWAP UDPLite を有効または無効にするには、**config ipv6 capwap** コマンドを使用します。

config ipv6 capwap udplite {**enable** | **disable**} [**all** | **<Cisco AP>**]

構文の説明

udplite	CAPWAP UDP Lite の IPv6 を設定します。
enable	IPv6 の CAPWAP UDP Lite を有効にします。
disable	IPv6 の CAPWAP UDP Lite を無効にします。
all	すべての Cisco AP で IPv6 の CAPWAP UDP Lite を有効または無効にします。
<Cisco AP>	ユーザが定義した Cisco AP で IPv6 の CAPWAP UDP Lite を有効または無効にします。

コマンド デフォルト

config ipv6 capwap udplite コマンドは、デフォルトでは **enabled** に設定されています。

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

使用上のガイドライン

- IPv6 の CAPWAP UDP Lite の設定は、IPv6 トンネルを使用してコントローラに接続されている AP だけに適用されます。
- IPv4 トンネルを使用して WLC に接続されている AP の場合、IPv6 の CAPWAP UDPLite のコマンドは、グローバル設定にも AP ごとにも適用されません。
- IPv6 には UDP の完全なペイロード チェックサムが必要です。これにより、パフォーマンスが影響を受けます。影響を最小限に抑えるために、データ トラフィックには UDPLite（ヘッダー チェックサムだけが必要）が使用され、制御トラフィックには UDP が使用されます。
- UDP Lite の使用はファイアウォールに影響します。中間ファイアウォールは、UDP Lite プロトコル（プロトコル ID 136）のパケットを許可するように設定する必要があります。
- UDP Lite をオフにすると、パケット処理においてパフォーマンス上の問題が発生します。
- UDP から UDPLite へ、またはその逆に変更する場合、AP は参加解除と再参加を強制されます。

次に、すべての Cisco AP または特定の Cisco AP で IPv6 の CAPWAP UDP Lite を設定する例を示します。

```
(Cisco Controller) >config ipv6 capwap udplite enable all
Changing AP's IPv6 Capwap UDP Lite mode will cause the AP to rejoin.
Are you sure you want to continue? (y/n)
```

config ipv6 interface

IPv6 システム インターフェイスを設定するには、**config ipv6 interface** コマンドを使用します。

config ipv6 interface {**acl** | **address** | **slaac**}

config ipv6 interface acl management *acl_name*

config ipv6 interface address {**management primary** *ipv6_address prefix_length ipv6_gateway_address* | **service-port** *ipv6_address prefix-length*}

config ipv6 interface slacc service-port［**enable** | **disable**］

構文の説明

acl	インターフェイスのアクセス コントロール リストで IPv6 を設定します。
management	管理インターフェイスを設定します。
acl_name	管理 ACL の IPv6 ACL 名を入力します。最大 32 文字の英数字で指定できます。
address	インターフェイスのアドレス情報で IPv6 を設定します。
management	管理インターフェイスを設定します。
primary	インターフェイスのプライマリ IPv6 アドレスを設定します。
ipv6_address	IPv6 アドレス情報でインターフェイスを設定します。
prefix_length	IPv6 プレフィックス長を設定します。プレフィックス長の範囲は 1 ー 127 です。
ipv6_gateway_address	リンク層 IPv6 ゲートウェイ アドレスを設定します。
service-port	アウトオブバンド サービス ポートで IPv6 を設定します。
ipv6_address	IPv6 アドレス情報でインターフェイスを設定します。
prefix_length	IPv6 プレフィックス長を設定します。プレフィックス長の範囲は 1 ー 127 です。

slacc	インターフェイスでSLAACオプションを設定します。
service-port	アウトオブバンド サービス ポートで IPv6 を設定します。
enable	SLAAC オプションを有効にします。
disable	SLAAC オプションを無効にします。

コマンド デフォルト

なし。

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

次に、IPv6 ACL 管理インターフェイスを設定する例を示します。

```
(Cisco Controller) >config ipv6 interface acl management Test_ACL
```

次に、IPv6 アドレスとプライマリ インターフェイスを設定する例を示します。

```
(Cisco Controller) > config ipv6 interface address management primary 2001:9:10:56::44
64 fe80::aea0:16ff:fe4f:2244
```

関連コマンド

show interface detailed management

show ipv6 interface summary

config ipv6 interface multicast

IPv6 マルチキャストを設定するには、**config ipv6 multicast** コマンドを使用します。

config ipv6 multicast mode {**unicast** | **multicast** *ipv6_address*}

構文の説明

mode	コントローラを AP マルチキャストまたはブロードキャスト IPv6 トラフィック転送モードに設定します。
unicast	マルチキャスト/ブロードキャスト IPv6 パケットは、AP へのユニキャスト CAPWAP トンネルにカプセル化されます。
multicast	マルチキャスト/ブロードキャスト IPv6 パケットは、AP へのマルチキャスト CAPWAP トンネルにカプセル化されます。
ipv6_address	IPv6 マルチキャスト アドレスを設定します。

コマンド デフォルト

- Cisco WLC 8500 および Cisco WLC 2500 ではマルチキャストがデフォルトで有効になっています。
- Cisco WLC 5500 ではユニキャストがデフォルトで有効になっています。

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

使用上のガイドライン

ありません。

次に、アクセスを許可するように Cisco WLC で IPv6 マルチキャストを設定する例を示します。

```
(Cisco Controller) >config ipv6 multicast 2001:DB8:0000:0000:0000:0000:0000:0001
```

次に、アクセスを許可するように Cisco WLC で IPv6 ユニキャストを設定する例を示します。

```
(Cisco Controller) > config ipv6 multicast mode unicast
```

関連コマンド

show network summary

config ipv6 neighbor-binding

シスコのワイヤレス LAN コントローラでネイバー バインディング テーブルを設定するには、**config ipv6 neighbor-binding** コマンドを使用します。

config ipv6 neighbor-binding {**timers** {**down-lifetime** *down_time* | **reachable-lifetime** *reachable_time* | **stale-lifetime** *stale_time* } | { **ra-throttle** {**allow at-least** *at_least_value*} | **enable** | **disable** | **interval-option** { **ignore** | **passthrough** | **throttle** } | **max-through** {*no_mcast_RA* | **no-limit**} | **throttle-period** *throttle_period*} }

構文の説明

timers	ネイバー バインディング テーブルのタイムアウト タイマーを設定します。
down-lifetime	ダウン ライフタイムを設定します。
down_time	秒単位のダウン ライフタイム。指定できる範囲は 0 ～ 86400 です。デフォルトは 30 秒です。
reachable-lifetime	到達可能なライフタイムを設定します。
reachable_time	秒単位の到達可能なライフタイム。指定できる範囲は 0 ～ 86400 です。デフォルトは 300 秒です。
stale-lifetime	古いライフタイムを設定します。
stale_time	秒単位の古いライフタイム。指定できる範囲は 0 ～ 86400 です。デフォルトは 86400 秒です。
ra-throttle	IPv6 RA スロットリング オプションを設定します。
allow	スロットル期間ごとに、ルータ 1 台あたりのマルチキャスト RA の数を指定します。
at_least_value	スロットリング前のルータからのマルチキャスト RA 数。有効な範囲は 0 ～ 32 です。デフォルトは 1 です。
enable	IPv6 RA スロットリングをイネーブルにします。
disable	IPv6 RA スロットリングをディセーブルにします。

interval-option	RFC3775 間隔オプションで RA の動作を調整します。
ignore	間隔オプションが、スロットリングに影響しないことを示します。
passthrough	RFC3775 間隔オプションですべての RA が転送されることを示します（デフォルト）。
throttle	RFC3775 間隔オプションですべての RA がスロットルされることを示します。
max-through	スロットル期間ごとに、VLANあたりのスロットルされない RA の数を指定します。
no_mcast_RA	スロットルを適用にする VLAN のマルチキャスト RA の数。vlan のデフォルト マルチキャスト RA は、10 です。
no-limit	VLAN レベルで、上限を設定しません。
throttle-period	スロットル期間を設定します。
throttle_period	秒単位のスロットル期間の長さ。範囲は10～86400 秒です。デフォルトは 600 秒です。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ネイバー バインディング テーブルを設定する例を示します。

```
(Cisco Controller) >config ipv6 neighbor-binding ra-throttle enable
```

関連コマンド

show ipv6 neighbor-binding

config ipv6 na-mcast-fwd

ネイバー アドバタイズメント マルチキャスト転送を設定するには、**config ipv6 na-mcast-fwd** コマンドを使用します。

config ipv6 na-mcast-fwd {**enable** | **disable**}

構文の説明

enable	ネイバーアドバタイズメントマルチキャスト転送を有効にします。
disable	ネイバーアドバタイズメントマルチキャスト転送を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

ネイバー アドバタイズメント マルチキャスト転送を有効にすると、有線またはワイヤレスからのすべての未承認マルチキャスト ネイバー アドバタイズメントがワイヤレスに転送されなくなります。

ネイバー アドバタイズメント マルチキャスト転送を無効にすると、コントローラの IPv6 重複アドレス検出（DAD）が影響を受けます。

次に、ネイバー アドバタイズメント マルチキャスト転送を設定する例を示します。

```
(Cisco Controller) >config ipv6 na-mcast-fwd enable
```

config ipv6 ns-mcast-fwd

ノンストップ マルチキャスト キャッシュ ミス転送を設定するには、**config ipv6 ns-mcast-fwd** コマンドを使用します。

config ipv6 ns-mcast-fwd {**enable** | **disable**}

構文の説明

enable	キャッシュ ミス時のノンストップ マルチキャスト転送を有効にします。
disable	キャッシュ ミス時のノンストップ マルチキャスト転送を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ノンストップ マルチキャスト転送を設定する例を示します。

```
(Cisco Controller) >config ipv6 ns-mcast-fwd enable
```

config ipv6 ra-guard

AP でクライアントから発信されるルータ アドバタイズメント（RA）パケットのフィルタ処理を設定するには、**config ipv6 ra-guard** コマンドを使用します。

config ipv6 ra-guard ap {**enable** | **disable**}

構文の説明

enable	AP で RA ガードを有効にします。
disable	AP で RA ガードを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IPv6 RA ガードを有効にする例を示します。

```
(Cisco Controller) >config ipv6 ra-guard enable
```

関連コマンド

show ipv6 ra-guard

config ipv6 route

IPv6 ネットワーク ルートを追加または削除するには、**config ipv6 route** コマンドを使用します。

config ipv6 route {**add** *network_ipv6_addr prefix-len ipv6_gw_addr* | **delete** *network _ipv6 addr* }

構文の説明

add	IPv6 ネットワーク ルートを追加します。
network_ipv6_addr	ネットワークの IPv6 アドレスを入力します。
prefix-len	ネットワークのプレフィックス長を入力します。
ipv6_gw_addr	システム インターフェイスを設定します。
delete	IPv6 ネットワーク ルートを削除します。
network_ipv6_addr	ネットワークの IPv6 アドレスを入力します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

使用上のガイドライン

- このコマンドは、異なるネットワークから IPv6 経由でサービス インターフェイスにアクセスするための IPv6 ネットワーク ルートを追加および削除するために使用されます。
- IPv6 ルートの追加中は、IPv6 ゲートウェイ アドレスがリンク ローカル スコープ（FE80::/64）である必要があります。

次に、IPv6 ルートを追加する例を示します。

```
(Cisco Controller) > config ipv6 route add 3010:1111:2222:abcd:abcd:abcd:abcd:1111 64
fe80::6616:8dff:fed3:c0cf
```

次に、IPv6 ルートを削除する例を示します。

```
(Cisco Controller) > config ipv6 route delete 2001:9:5:90::115
```

関連コマンド

show ipv6 route summary

config コマンド：j ～ q

- config known ap （549 ページ）
- config lag （550 ページ）
- config ldap （551 ページ）
- config local-auth active-timeout （553 ページ）
- config local-auth cipher-option （554 ページ）
- config local-auth eap-profile （555 ページ）
- config local-auth method fast （558 ページ）
- config local-auth user-credentials （560 ページ）
- config lync-sdn （561 ページ）
- config licensing （562 ページ）
- config license boot （563 ページ）
- config load-balancing （565 ページ）
- config location （567 ページ）
- config location info rogue （570 ページ）
- config logging buffered （571 ページ）
- config logging console （572 ページ）
- config logging debug （573 ページ）
- config logging fileinfo （574 ページ）
- config logging procinfo （575 ページ）
- config logging traceinfo （576 ページ）
- config logging syslog host （577 ページ）
- config logging syslog facility （580 ページ）
- config logging syslog facility client （584 ページ）
- config logging syslog facility ap （585 ページ）
- config logging syslog level （586 ページ）
- config loginsession close （587 ページ）
- config macfilter （588 ページ）
- config macfilter description （590 ページ）
- config macfilter interface （591 ページ）

- config macfilter ip-address （592 ページ）
- config macfilter mac-delimiter （593 ページ）
- config macfilter radius-compat （594 ページ）
- config macfilter wlan-id （595 ページ）
- config mdns ap （596 ページ）
- config mdns profile （598 ページ）
- config mdns query interval （600 ページ）
- config mdns service （601 ページ）
- config mdns snooping （604 ページ）
- config mdns policy enable （605 ページ）
- config mdns policy service-group （606 ページ）
- config mdns policy service-group parameters （607 ページ）
- config mdns policy service-group user-name （608 ページ）
- config mdns policy service-group user-role （609 ページ）
- config media-stream multicast-direct （610 ページ）
- config media-stream message （611 ページ）
- config media-stream add （613 ページ）
- config media-stream admit （615 ページ）
- config media-stream deny （616 ページ）
- config media-stream delete （617 ページ）
- config memory monitor errors （618 ページ）
- config memory monitor leaks （619 ページ）
- config mesh alarm （621 ページ）
- config mesh astools （623 ページ）
- config mesh backhaul rate-adapt （624 ページ）
- config mesh backhaul slot （626 ページ）
- config mesh battery-state （627 ページ）
- config mesh client-access （628 ページ）
- config mesh convergence （630 ページ）
- config mesh ethernet-bridging allow-bpdu （631 ページ）
- config mesh ethernet-bridging vlan-transparent （632 ページ）
- config mesh full-sector-dfs （633 ページ）
- config mesh linkdata （634 ページ）
- config mesh linktest （637 ページ）
- config mesh lsc （640 ページ）
- config mesh lsc advanced （641 ページ）
- config mesh lsc advanced ap-provision （642 ページ）
- config mesh multicast （643 ページ）
- config mesh parent preferred （645 ページ）
- config mesh public-safety （646 ページ）
- config mesh radius-server （647 ページ）

- config mesh range （648 ページ）
- config mesh secondary-backhaul （649 ページ）
- config mesh security （650 ページ）
- config mesh slot-bias （652 ページ）
- config mgmtuser add （653 ページ）
- config mgmtuser delete （654 ページ）
- config mgmtuser description （655 ページ）
- config mgmtuser password （656 ページ）
- config mgmtuser telnet （657 ページ）
- config mgmtuser termination-interval （658 ページ）
- config mobility dscp （659 ページ）
- config mobility group anchor （660 ページ）
- config mobility group domain （661 ページ）
- config mobility group keepalive count （662 ページ）
- config mobility group keepalive interval （663 ページ）
- config mobility group member （664 ページ）
- config mobility group multicast-address （666 ページ）
- config mobility multicast-mode （667 ページ）
- config mobility new-architecture （668 ページ）
- config mobility oracle （669 ページ）
- config mobility secure-mode （670 ページ）
- config mobility statistics reset （671 ページ）
- config netuser add （672 ページ）
- config netuser delete （674 ページ）
- config netuser description （675 ページ）
- config netuser guest-lan-id （676 ページ）
- config netuser guest-role apply （677 ページ）
- config netuser guest-role create （678 ページ）
- config netuser guest-role delete （679 ページ）
- config netuser guest-role qos data-rate average-data-rate （680 ページ）
- config netuser guest-role qos data-rate average-realtime-rate （681 ページ）
- config netuser guest-role qos data-rate burst-data-rate （682 ページ）
- config netuser guest-role qos data-rate burst-realtime-rate （683 ページ）
- config netuser lifetime （684 ページ）
- config netuser maxUserLogin （685 ページ）
- config netuser password （686 ページ）
- config netuser wlan-id （687 ページ）
- config network client-ip-conflict-detection （688 ページ）
- config network bridging-shared-secret （689 ページ）
- config network web-auth captive-bypass （690 ページ）
- config network web-auth port （691 ページ）

- config network web-auth proxy-redirect （692 ページ）
- config network web-auth secureweb （693 ページ）
- config network webmode （694 ページ）
- config network web-auth （695 ページ）
- config network 802.3-bridging （696 ページ）
- config network allow-old-bridge-aps （697 ページ）
- config network ap-discovery （698 ページ）
- config network ap-fallback （699 ページ）
- config network ap-priority （700 ページ）
- config network apple-talk （701 ページ）
- config network arptimeout （702 ページ）
- config assisted-roaming （703 ページ）
- config network bridging-shared-secret （704 ページ）
- config network broadcast （705 ページ）
- config network fast-ssid-change （706 ページ）
- config network ip-mac-binding （707 ページ）
- config network link local bridging （708 ページ）
- config network master-base （709 ページ）
- config network mgmt-via-wireless （710 ページ）
- config network multicast global （711 ページ）
- config network multicast igmp query interval （712 ページ）
- config network multicast igmp snooping （713 ページ）
- config network multicast igmp timeout （714 ページ）
- config network multicast l2mcast （715 ページ）
- config network multicast mld （716 ページ）
- config network multicast mode multicast （717 ページ）
- config network multicast mode unicast （718 ページ）
- config network oeap-600 dual-rlan-ports （719 ページ）
- config network oeap-600 local-network （720 ページ）
- config network otap-mode （721 ページ）
- config network profiling （722 ページ）
- config pmipv6 domain （723 ページ）
- config pmipv6 add profile （724 ページ）
- config pmipv6 delete （725 ページ）
- config pmipv6 mag apn （726 ページ）
- config pmipv6 mag binding init-retx-time （727 ページ）
- config pmipv6 mag binding lifetime （728 ページ）
- config pmipv6 mag binding max-retx-time （729 ページ）
- config pmipv6 mag binding maximum （730 ページ）
- config pmipv6 mag binding refresh-time （731 ページ）
- config pmipv6 mag bri delay （732 ページ）

- config pmipv6 mag bri retries （733 ページ）
- config pmipv6 mag lma （734 ページ）
- config pmipv6 mag replay-protection （735 ページ）
- config port power （736 ページ）
- config network rf-network-name （737 ページ）
- config network secureweb （738 ページ）
- config network secureweb cipher-option （739 ページ）
- config network ssh （741 ページ）
- config network telnet （742 ページ）
- config network usertimeout （743 ページ）
- config network web-auth captive-bypass （744 ページ）
- config network web-auth cmcc-support （745 ページ）
- config network web-auth port （746 ページ）
- config network web-auth proxy-redirect （747 ページ）
- config network web-auth secureweb （748 ページ）
- config network web-auth https-redirect （749 ページ）
- config network webcolor （750 ページ）
- config network webmode （751 ページ）
- config network web-auth （752 ページ）
- config network zero-config （753 ページ）
- config network allow-old-bridge-aps （754 ページ）
- config network ap-discovery （755 ページ）
- config network ap-fallback （756 ページ）
- config network ap-priority （757 ページ）
- config network apple-talk （758 ページ）
- config network bridging-shared-secret （759 ページ）
- config network master-base （760 ページ）
- config network oeap-600 dual-rlan-ports （761 ページ）
- config network oeap-600 local-network （762 ページ）
- config network otap-mode （763 ページ）
- config network zero-config （764 ページ）
- config nmsp notify-interval measurement （765 ページ）
- config paging （766 ページ）
- config passwd-cleartext （767 ページ）
- config policy （768 ページ）
- config port adminmode （771 ページ）
- config port autoneg （772 ページ）
- config port linktrap （773 ページ）
- config port multicast appliance （774 ページ）
- config prompt （775 ページ）
- config qos average-data-rate （776 ページ）

- config qos average-realtime-rate （778 ページ）
- config qos burst-data-rate （780 ページ）
- config qos burst-realtime-rate （782 ページ）
- config qos description （784 ページ）
- config qos max-rf-usage （785 ページ）
- config qos dot1p-tag （786 ページ）
- config qos priority （787 ページ）
- config qos protocol-type （789 ページ）
- config qos queue_length （790 ページ）
- config qos qosmap （791 ページ）
- config qos qosmap up-to-dscp-map （792 ページ）
- config qos qosmap dscp-to-up-exception （793 ページ）
- config qos qosmap delete-dscp-exception （794 ページ）
- config qos qosmap clear-all （795 ページ）
- config qos qosmap trust dscp upstream （796 ページ）

config known ap

既知の Cisco Lightweight アクセス ポイントを設定するには、**config known ap** コマンドを使用します。

config known ap {**add** | **alert** | **delete**} *MAC*

構文の説明

add	新しい既知のアクセス ポイント エントリを追加します。
alert	アクセス ポイントの検出時にトラップを生成します。
delete	既存の既知のアクセス ポイント エントリを削除します。
MAC	既知の Cisco Lightweight アクセス ポイントの MAC アドレス。

コマンド デフォルト

なし

次に、新しいアクセス ポイント エントリ ac:10:02:72:2f:bf を既知のアクセス ポイントに追加する例を示します。

```
(Cisco Controller) >config known ap add ac:10:02:72:2f:bf 12
```

config lag

リンク集約（LAG）を有効または無効にするには、**config lag** コマンドを使用します。

config lag {**enable** | **disable**}

構文の説明

enable	リンク集約（LAG）設定を有効にします。
disable	リンク集約（LAG）設定を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、LAG 設定を有効にする例を示します。

```
(Cisco Controller) > config lag enable
Enabling LAG will map your current interfaces setting to LAG interface,
All dynamic AP Manager interfaces and Untagged interfaces will be deleted
All WLANs will be disabled and mapped to Mgmt interface
Are you sure you want to continue? (y/n)
You must now reboot for the settings to take effect.
```

次に、LAG 設定を無効にする例を示します。

```
(Cisco Controller) > config lag disable
Disabling LAG will map all existing interfaces to port 1.
Are you sure you want to continue? (y/n)
You must now reboot for the settings to take effect.
```

config ldap

Lightweight Directory Access Protocol（LDAP）サーバの設定を行うには、**config ldap** コマンドを使用します。

config ldap {**add** | **delete** | **enable** | **disable** | **retransmit-timeout** | **retry** | **user** | **security-mode** | **simple-bind**} *index*

config ldap add *index server_ip_address port user_base user_attr user_type* [**secure**]

config ldap retransmit-timeout *index retransmit-timeout*

config ldap retry *attempts*

config ldap user {**attr** *index user-attr* | **base** *index user-base* | **type***index user-type*}

config ldap security-mode {**enable** | **disable**}*index*

config ldap simple-bind {**anonymous** *index* | **authenticated** *index username password*}

構文の説明

add	LDAP サーバの追加を指定します。
delete	LDAP サーバの削除を指定します。
enable	LDAP サーバの有効化を指定します。
disable	LDAP サーバの無効化を指定します。
retransmit-timeout	LDAP サーバのデフォルト再送信タイムアウトを変更します。
retry	LDAP サーバの再試行回数を設定します。
user	ユーザ検索パラメータを設定します。
security-mode	セキュリティ モードを設定します。
simple-bind	ローカル認証バインド方式を設定します。
anonymous	LDAPサーバへの匿名アクセスを許可します。
authenticated	LDAP サーバに安全にアクセスのため、ユーザ名とパスワードを入力することを指定します。
index	LDAP サーバインデックス。範囲は 1 ～ 17 です。
server_ip_address	LDAP サーバの IP アドレス。

port	ポート番号。
user_base	すべてのユーザを含むサブツリーの識別名。
user_attr	ユーザ名を含む属性。
user_type	ユーザを識別するオブジェクト タイプ。
secure	（任意）Transport Layer Security（TLS）を使用することを指定します。
retransmit-timeout	LDAP サーバの再送信タイムアウト。指定できる範囲は 2 ～ 30 です。
attempts	各 LDAP サーバを再試行する回数。
attr	ユーザ名を含む属性を設定します。
base	すべてのユーザを含むサブツリーの識別名を設定します。
type	ユーザ タイプを設定します。
username	認証されたバインド方式のユーザ名。
password	認証されたバインド方式のパスワード。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
7.6	セキュア LDAP をサポートするために **secure** キーワードが追加されました。

使用上のガイドライン

セキュア LDAP を有効にすると、コントローラはサーバ証明書を検証しなくなります。

次に、LDAP サーバ インデックス 10 を有効にする例を示します。

```
(Cisco Controller) > config ldap enable 10
```

関連コマンド

config ldap add

config ldap simple-bind

show ldap summary

config local-auth active-timeout

設定済みのRADIUSサーバのペアによる認証が失敗した後に、コントローラがローカル拡張認証プロトコル（EAP）を使用してワイヤレスクライアントの認証を試行する時間を指定するには、**config local-auth active-timeout** コマンドを使用します。

config local-auth active-timeout *timeout*

構文の説明

timeout	タイムアウト時間を秒単位で指定します。有効な範囲は 1 ～ 3600 です。

コマンド デフォルト

デフォルトのタイムアウト値は 100 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、EAPを使用して、ワイヤレスクライアントを認証するためのアクティブ タイムアウトを 500 秒に指定する例を示します。

```
(Cisco Controller) > config local-auth active-timeout 500
```

関連コマンド

clear stats local-auth

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth cipher-option

3des-rc4 暗号オプションを設定するには、**config local-auth cipher-option** コマンドを使用します。

config local-auth cipher-option {**enable** | **disable** }

構文の説明

cipher-option	暗号オプションを設定します。
enable	3des-rc4 暗号を有効にすることを許可します。
disable	3des-rc4 暗号を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、WLC で暗号オプションを無効にする例を示します。

```
(Cisco Controller) > config local-auth cipher-option 3des-rc4 disable
```

config local-auth eap-profile

ローカル拡張可能認証プロトコル（EAP）認証プロファイルを設定するには、**config local-auth eap-profile** コマンドを使用します。

config local-auth eap-profile {[**add** | **delete**] *profile_name* | **cert-issuer** {**cisco** | **vendor**} | **method** *method* **local-cert** {**enable** | **disable**} *profile_name* | **method** *method* **client-cert** {**enable** | **disable**} *profile_name* | **method** *method* **peer-verify ca-issuer** {**enable** | **disable**} | **method** *method* **peer-verify cn-verify** {**enable** | **disable**} | **method** *method* **peer-verify date-valid** {**enable** | **disable**}

構文の説明

add	（任意）EAP プロファイルまたは方式の追加を指定します。
delete	（任意）EAP プロファイルまたは方式の削除を指定します。
profile_name	EAP プロファイル名（最大 63 文字の英数字）。プロファイル名にはスペースは使用できません。
cert-issuer	（Extensible Authentication Protocol Transport Layer Security（EAP-TLS）、Protected Extensible Authentication Protocol（PEAP）、または Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）と証明書を使用している場合）クライアントに送信される証明書の発行元を指定します。証明書発行元としてはCiscoまたはサードパーティ ベンダーがサポートされています。
cisco	シスコの証明書の発行元を指定します。
vendor	サード パーティ ベンダーを指定します。
method	EAP プロファイル方式を設定します。
method	EAP プロファイル方式名。サポートされている方式は leap、fast、tls、および peap です。
local-cert	（EAP-FAST で使用する場合）認証のために、コントローラ上にデバイス証明書が必要かどうかを指定します。
enable	パラメータ ID の有効化を指定します。
disable	パラメータ ID の無効化を指定します。

client-cert	（EAP-FAST で使用する場合）認証用のデバイス証明書をコントローラへ送信するために、無線クライアントが必要かどうかを指定します。
peer-verify	ピア証明書検証オプションを設定します。
ca-issuer	（EAP-TLS または EAP-FAST と証明書を使用している場合）クライアントから受信した証明書を、コントローラ上の認証局（CA）の証明書と照合するかどうかを指定します。
cn-verify	（EAP-TLS または EAP-FAST と証明書を使用している場合）受信した証明書の通常名（CN）をコントローラ上の CA 証明書の CN と照合するかどうかを指定します。
date-valid	（EAP-TLS または EAP-FAST と証明書を使用している場合）受信したデバイス証明書が有効で期限切れになっていないことをコントローラで検証するかどうかを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FAST01 という名前のローカル EAP プロファイルを作成する例を示します。

```
(Cisco Controller) > config local-auth eap-profile add FAST01
```

次に、ローカル EAP プロファイルに EAP-FAST 方式を追加する例を示します。

```
(Cisco Controller) > config local-auth eap-profile method add fast FAST01
```

次に、EAP-FAST プロファイルのクライアントに送信される証明書の発行元としてシスコを指定する例を示します。

```
(Cisco Controller) > config local-auth eap-profile method fast cert-issuer cisco
```

次に、クライアントから受信する証明書がコントローラ上の CA 証明書と照合されるように指定する例を示します。

```
(Cisco Controller) > config local-auth eap-profile method fast peer-verify ca-issuer
enable
```

関連コマンド

config local-auth active-timeout

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth method fast

EAP-FASTプロファイルを設定するには、**config local-auth method fast** コマンドを使用します。

config local-auth method fast {**anon-prov** [**enable** | **disable**] | **authority-id** *auth_id* **pac-ttl** *days* | **server-key** *key_value*}

構文の説明

anon-prov	匿名プロビジョニングが可能なようにコントローラを設定します。これにより、Protected Access Credential（PAC）プロビジョニング中に、PACを持たないクライアントにPACを自動的に送信できるようになります。
enable	（任意）パラメータを有効化することを指定します。
disable	（任意）パラメータを無効化することを指定します。
authority-id	ローカルEAP-FASTサーバの権限識別子を設定します。
auth_id	ローカルEAP-FASTサーバの権限識別子（2～32の16進数値）。
pac-ttl	Protected Access Credential（PAC）の有効期間の日数を設定します。これは存続可能時間（TTL）値とも呼ばれます。
days	存続可能時間（TTL）の値（1～1000日）。
server-key	PACを暗号化または復号化するサーバ キーを設定します。
key_value	暗号キーの値（2～32の16進数値）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、匿名プロビジョニングを許可するためにコントローラを無効にする例を示します。

```
(Cisco Controller) > config local-auth method fast anon-prov disable
```

次に、ローカルEAP-FASTサーバの権限識別子0125631177を設定する例を示します。

```
(Cisco Controller) > config local-auth method fast authority-id 0125631177
```

次に、PACの有効日数を10日に設定する例を示します。

```
(Cisco Controller) > config local-auth method fast pac-ttl 10
```

関連コマンド

clear stats local-auth

config local-auth eap-profile

config local-auth active-timeout

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth user-credentials

ユーザ クレデンシャルをローカル拡張可能認証プロトコル（EAP）認証データベースで検索する順序を設定するには、**config local-auth user credentials** コマンドを使用します。

config local-auth user-credentials ｛**local**［**ldap**］ | **ldap**［**local**］ ｝

構文の説明

local	ユーザ クレデンシャルをローカル データベースで検索することを指定します。
ldap	（任意）ユーザ クレデンシャルを Lightweight Directory Access Protocol（LDAP）データベースで検索することを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

特定のデータベース パラメータの順序は、データベースの検索順序を示します。

次に、ローカル EAP 認証データベースが検索される順序を指定する例を示します。

```
(Cisco Controller) > config local-auth user credentials local lda
```

上記の例では、最初にローカル データベースが検索され、次に LDAP データベースが検索されます。

関連コマンド

clear stats local-auth

config local-auth eap-profile

config local-auth method fast

config local-auth active-timeout

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config lync-sdn

Lync サービスを設定するには、 **config lync-sdn** コマンドを使用します。

config lync-sdn {**port** *port-number*} | {**enable** | **disable**}

構文の説明

port	Lync サーバ ポート番号を設定します。
port-number	サーバのポート番号。
enable	Lyncサービスをグローバルに有効にします。
disable	Lyncサービスをグローバルに無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、Lync サービスをグローバルに有効にする例を示します。

```
(Cisco Controller) >config lync-sdn enable
```

config licensing

シスコ スマート ソフトウェア ライセンシングと RTU ライセンス プラットフォームを切り替えるには、**config licensing** コマンドを使用します。

config licensing {**rtu** | **smart-license**} **dns-server** *ip address*

構文の説明

rtu	使用権（RTU）ライセンスプラットフォーム。
smart-license	シスコ スマート ソフトウェア ライセンシング。
dns-server	スマート ソフトウェア ライセンシングの DNS サーバ パラメータを設定します。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

コマンド デフォルト

使用権（RTU）が、デバイスのデフォルトのライセンス メカニズムです。

次に、コントローラでシスコ スマート ソフトウェア ライセンシングをアクティブにする例を示します。

```
(Cisco Controller) > config licensing smart-license dns-server 209.165.200.224
```

（注） ライセンス プラットフォームの変更をアクティブにするにはコントローラを再起動する必要があります。

config license boot

Cisco 5500 シリーズのコントローラの次回リブート時に使用するライセンス レベルを指定するには、**config license boot** コマンドを使用します。

config license boot {**base** | **wplus** | **auto**}

構文の説明

base	base ブート レベルを指定します。
wplus	wplus ブート レベルを指定します。
auto	auto ブート レベルを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

auto を入力すると、ライセンス ソフトウェアは、次回リブート時に使用するライセンス レベルを自動的に選択します。通常、評価ライセンスよりも永久ライセンスのほうが優先されます。また、ベース ライセンスよりも WPLUS ライセンスのほうが優先されます。

（注） ベース ライセンスから WPLUS ライセンスへのアップグレードを検討している場合、WPLUS 評価ライセンスを試してから WPLUS 永久ライセンスにアップグレードできます。評価ライセンスをアクティブ化するには、ベース永久ライセンスではなく WPLUS 評価ライセンスがコントローラで使用されるように、イメージ レベルを設定する必要があります。

（注） 操作の中断を避けるために、コントローラは、評価ライセンスの有効期限が切れてもライセンスを切り替えません。永久ライセンスに戻すには、コントローラをリブートする必要があります。リブート後に、期限切れになった評価ライセンスと同じフィーチャ セット レベルにコントローラがデフォルト設定されます。同じフィーチャ セット レベルの永久ライセンスがインストールされていない場合、コントローラは、別のレベルの永久ライセンスまたは有効期限の切れていない評価ライセンスを使用します。

次に、ライセンスのブート設定を wplus に設定する例を示します。

```
(Cisco Controller) > config license boot wplus
```

関連コマンド

license install

show license in-use

license modify priority

config load-balancing

アグレッシブなロード バランシングをコントローラでグローバルに設定するには、**config load-balancing** コマンドを使用します。

config load-balancing {**window** *client_count* | **status** {**enable** | **disable**} | **denial** *denial_count*}

config load-balancing uplink-threshold *traffic_threshold*

構文の説明

window	アグレッシブなロードバランシング クライアント ウィンドウを指定します。
client_count	1 ～ 20 のクライアントを含む、アグレッシブなロードバランシング クライアント ウィンドウ。
status	ロード バランシングの状態を設定します。
enable	ロード バランシング機能をイネーブルにします。
disable	ロード バランシング機能をディセーブルにします。
denial	ロードバランシング時に拒否されるアソシエーションの数を指定します。
denial_count	ロード バランシング中のアソシエーション拒否の最大数（0 ～ 10）。
uplink-threshold	アクセス ポイントが新しいアソシエーションを拒否できるように、しきい値のトラフィックを指定します。
traffic_threshold	アクセス ポイントが新しいアソシエーションを拒否するためのしきい値のトラフィック。この値は、90 秒間隔で測定された WAN 使用率のパーセントです。たとえば、デフォルトしきい値が 50 である場合、アクセス ポイント WAN インターフェイスで 50% 以上の使用率が検出されると、ロード バランシングがトリガされます。

コマンド デフォルト

デフォルトでは、アグレッシブなロード バランシングは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

負荷分散が有効になっている WLAN は、音声およびビデオなどの時間依存型アプリケーションをサポートしません。これは、ローミングでの遅延が存在するためです。

コントローラとともに Cisco 7921 および 7920 Wireless IP Phone を使用する場合、各コントローラの音声 WLAN でアグレッシブなロードバランシングが無効化されていることを確認します。無効化されていない場合、電話による初期ローミングが失敗し、オーディオパスが中断されることがあります。

クライアントをロードバランシングできるのは、同じコントローラに接続されているアクセスポイントのみです。WAN 使用率は次の式を使用してパーセントとして産出されます: (送信されたデータ レート (1 秒あたり) + 受信したデータ レート (1 秒あたり))/(1000Mbps TX + 1000Mbps RX) * 100

次に、アグレッシブなロード バランシングの設定を有効にする例を示します。

```
(Cisco Controller) > config load-balancing aggressive enable
```

関連コマンド

show load-balancing

config wlan load-balance

config location

ロケーションベースのシステムを設定するには、**config location** コマンドを指定します。

config location {**algorithm** {**simple** | **rssi-average**} | {**rssi-half-life** | **expiry**} [**client** | **calibrating-client** | **tags** | **rogue-aps**] *seconds* | **notify-threshold** [**client** | **tags** | **rogue-aps**] *threshold* | **interface-mapping** {**add** | **delete**} *location wlan_id interface_name* | **plm** {**client** {**enable** | **disable**} *burst_interval* | **calibrating** {**enable** | **disable**} {**uniband** | **multiband**}}}

構文の説明

algorithm	（注） **config location algorithm** コマンドは使用も変更もしないでください。このコマンドは、最適なデフォルト値に設定されています。 平均 RSSI および SNR 値に使用されるアルゴリズムを設定します。
simple	必要とする CPU オーバーヘッドは小さいが精度が低い、高速アルゴリズムを指定します。
rssi-average	より正確なアルゴリズムが指定されますが、より多くの CPU オーバーヘッドが必要です。
rssi-half-life	（注） **config location rssi-half-life** コマンドは使用も変更もしないでください。このコマンドは、最適なデフォルト値に設定されています。 2 つの RSSI 測定値を平均するときに、半減期を設定します。
expiry	（注） **config location expiry** コマンドは使用も変更もしないでください。このコマンドは、最適なデフォルト値に設定されています。 RSSI 値のタイムアウトを設定します。
client	（任意）クライアント デバイスに適用するパラメータを指定します。
calibrating-client	（任意）調整クライアント デバイスに使用するパラメータを指定します。
tags	（任意）無線周波数 ID（RFID）タグに適用するパラメータを指定します。

rogue-aps	（任意）不正なアクセス ポイントに適用するパラメータを指定します。
seconds	秒数を指定します（0、1、2、5、10、20、30、60、90、120、180、300 秒）。
notify-threshold	（注） **config location notify-threshold** コマンドは使用も変更もしないでください。このコマンドは、最適なデフォルト値に設定されています。 RSSI 測定に NMSP 通知しきい値を指定します。
threshold	しきい値のパラメータ。範囲は 0 ～ 10 dB で、デフォルト値は 0 dB です。
interface-mapping	新規のロケーション、無線 LAN、またはインターフェイス マッピング要素を追加または削除します。
wlan_id	WLAN の識別名。
interface_name	マッピング要素を適用するインターフェイスの名前。
plm	通常のクライアントまたは調整クライアントのパス損失測定（S60）要求を指定します。
client	通常の、未調整のクライアントを指定します。
burst_interval	バースト間隔。有効範囲は 1 ～ 3600 秒で、デフォルト値は 60 秒です。
calibrating	調整クライアントを指定します。
uniband	関連付けられた 802.11a または 802.11b/g 無線を指定します（ユニバンド）。
multiband	関連付けられた 802.11a/b/g 無線を指定します（マルチバンド）。

コマンド デフォルト

個々の引数およびキーワードのデフォルト値については、「構文の説明」の項を参照してください。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ロケーション ベースのコントローラで RSSI 値および SNR 値を平均する単純なアルゴリズムを指定する例を示します。

```
(Cisco Controller) > config location algorithm simple
```

関連コマンド

config location info rogue

clear location rfid

clear location statistics rfid

show location

show location statistics rfid

config location info rogue

不正サービスの情報通知を設定するには、**config location info rogue** コマンドを使用します。

config location info rogue {**basic** | **extended**}

構文の説明

basic	不正情報通知サービスの基本不正パラメータ（mode、class、containmentlevel、numclients、firsttime、lasttime、ssid など）を設定します。 （注） Cisco MSE のバージョンが Cisco WLC のバージョンより古い場合は、基本パラメータを設定してください。
extended	不正情報通知サービスの拡張不正パラメータ（基本パラメータに加えて、セキュリティ タイプ、LRAD タイプ検出など）を設定します。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

config logging buffered

コントローラ バッファへのロギング メッセージの重大度を設定するには、**config logging buffered** コマンドを使用します。

config logging buffered `security_level`

構文の説明

security_level	セキュリティ レベル。次のいずれかを選択します。 • 緊急：重大度 0 • アラート：重大度 1 • 重要：重大度 2 • エラー：重大度 3 • 警告：重大度 4 • 通知：重大度 5 • 情報：重大度 6 • デバッグ：重大度 7

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ロギング メッセージに対するコントローラのバッファの重大度を 4 に設定する例を示します。

```
(Cisco Controller) > config logging buffered 4
```

関連コマンド

config logging syslog facility

config logging syslog level

show logging

config logging console

コントローラ コンソールへのロギング メッセージの重大度を設定するには、**config logging console** コマンドを使用します。

config logging console *security_level*

構文の説明

security_level	重大度。次のいずれかを選択します。 • 緊急：重大度 0 • アラート：重大度 1 • 重要：重大度 2 • エラー：重大度 3 • 警告：重大度 4 • 通知：重大度 5 • 情報：重大度 6 • デバッグ：重大度 7

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ロギング メッセージに対するコントローラのコンソールの重大度を 3 に設定する例を示します。

```
(Cisco Controller) > config logging console 3
```

関連コマンド

config logging syslog facility

config logging syslog level

show logging

config logging debug

デバッグ メッセージをコントローラ バッファ、コントローラ コンソール、または syslog サーバに保存するには、**config logging debug** コマンドを使用します。

config logging debug {**buffered** | **console** | **syslog**} {**enable** | **disable**}

構文の説明

buffered	コントローラ バッファにデバッグ メッセージを保存します。
console	コントローラ コンソールにデバッグ メッセージを保存します。
syslog	syslog サーバにデバッグ メッセージを保存します。
enable	デバッグ メッセージのロギングをイネーブルにします。
disable	デバッグ メッセージのロギングをディセーブルにします。

コマンド デフォルト

デフォルトでは、 **console** コマンドが有効になっており、 **buffered** コマンドと **syslog** コマンドが無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラ コンソールにデバッグ メッセージを保存する例を示します。

```
(Cisco Controller) > config logging debug console enable
```

関連コマンド

show logging

config logging fileinfo

コントローラがメッセージ ログ内にソース ファイルの情報を含めるようにする、またはこの情報を表示しないようにするには、**config logging fileinfo** コマンドを使用します。

config logging fileinfo {**enable** | **disable**}

構文の説明

enable	メッセージ ログにソース ファイルの情報を含めます。
disable	コントローラがメッセージ ログのソース ファイルの情報を表示しないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラがメッセージ ログにソース ファイルの情報を含めるようにする例を示します。

```
(Cisco Controller) > config logging fileinfo enable
```

関連コマンド

show logging

config logging procinfo

コントローラがメッセージ ログ内にプロセス情報を含めるようにする、またはこの情報を表示しないようにするには、**config logging procinfo** コマンドを使用します。

config logging procinfo {**enable** | **disable**}

構文の説明

enable	プロセス情報をメッセージ ログに含めます。
disable	コントローラがメッセージ ログにプロセス情報を表示しないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラがメッセージ ログにプロセス情報を含めるようにする例を示します。

```
(Cisco Controller) > config logging procinfo enable
```

関連コマンド

show logging

config logging traceinfo

コントローラがメッセージログ内にトレースバック情報を含めるようにする、またはこの情報を表示しないようにするには、**config logging traceinfo** コマンドを使用します。

config logging traceinfo {**enable** | **disable**}

構文の説明

enable	トレースバック情報をメッセージ ログに含めます。
disable	コントローラがメッセージログにトレースバック情報を表示しないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、コントローラがメッセージ ログにトレースバック情報を含めないようにする例を示します。

```
(Cisco Controller) > config logging traceinfo disable
```

関連コマンド

show logging

config logging syslog host

syslog メッセージを送信するためにリモート ホストを設定するには、**config logging syslog host** コマンドを使用します。

config logging syslog host *ip_addr*

構文の説明

ip_addr	リモート ホストの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

- syslog メッセージを送信するためにリモート ホストを設定するには、**config logging syslog host** *ip_addr* コマンドを使用します。
- syslog メッセージを送信するように設定されたリモート ホストを削除するには、**config logging syslog host** *ip_addr* **delete** コマンドを使用します。
- コントローラで設定されている syslog サーバを表示するには、**show logging** コマンドを使用します。

次に、syslog メッセージを送信するために 2 つのリモート ホスト（10.92.125.52 と 2001:9:6:40::623）を設定し、コントローラで設定されている syslog サーバを表示する例を示します。

```
(Cisco Controller) > config logging syslog host 10.92.125.52
System logs will be sent to 10.92.125.52 from now on

(Cisco Controller) > config logging syslog host 2001:9:6:40::623
System logs will be sent to 2001:9:6:40::623 from now on

(Cisco Controller) > show logging
Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level.......................... errors
 - Number of system messages logged.............. 1316
 - Number of system messages dropped............. 6892
- Logging of debug messages to buffer ........... Disabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
- Cache of logging  ............................. Disabled
- Cache of logging time(mins) ................... 10080
- Number of over cache time log dropped  ........ 0
Logging to console :
```

```
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8243
- Logging of debug messages to console ..... Enabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
Logging to syslog :
- Syslog facility..... local0
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8208
- Logging of debug messages to console ..... Enabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Logging of system messages to syslog :
 - Logging filter level..... errors
 - Number of system messages logged..... 1316
 - Number of system messages dropped..... 6892
- Logging of debug messages to syslog ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Number of remote syslog hosts..... 2
- syslog over tls..... Disabled
  - Host 0..... 10.92.125.52
  - Host 1..... 2001:9:6:40::623
  - Host 2.....
Logging of RFC 5424..... Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file..... Disabled
- Number of debug messages logged..... 0
- Number of debug messages dropped..... 0
Logging of traceback..... Enabled
```

次に、syslog メッセージを送信するために設定されている 2 つのリモート ホスト（10.92.125.52 と 2001:9:6:40::623）を削除し、設定されていた syslog サーバがコントローラから削除されたことを表示する例を示します。

```
(Cisco Controller) > config logging syslog host 10.92.125.52 delete
System logs will not be sent to 10.92.125.52 anymore

(Cisco Controller) > config logging syslog host 2001:9:6:40::623 delete
System logs will not be sent to 2001:9:6:40::623 anymore

(Cisco Controller) > show logging

Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level..... errors
 - Number of system messages logged..... 1316
 - Number of system messages dropped..... 6895
- Logging of debug messages to buffer ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Cache of logging  ..... Disabled
- Cache of logging time(mins) ..... 10080
- Number of over cache time log dropped  ..... 0
Logging to console :
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8211
```

```
- Logging of debug messages to console .......... Enabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
Logging to syslog :
- Syslog facility................................ local0
- Logging of system messages to syslog :
 - Logging filter level.......................... errors
 - Number of system messages logged.............. 1316
 - Number of system messages dropped............. 6895
- Logging of debug messages to syslog ........... Disabled
 - Number of debug messages logged............... 0
 - Number of debug messages dropped.............. 0
- Number of remote syslog hosts.................. 0
- syslog over tls................................ Disabled
  - Host 0.......................................
  - Host 1.......................................
  - Host 2.......................................
Logging of RFC 5424............................. Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file.............. Disabled
- Number of debug messages logged................ 0
- Number of debug messages dropped............... 0
Logging of traceback............................ Enabled
- Traceback logging level........................ errors
Logging of source file informational............. Enabled
Timestamping of messages.......................
- Timestamping of system messages................ Enabled
 - Timestamp format.............................. Date and Time
```

config logging syslog facility

リモート ホストへの発信 syslog メッセージのファシリティを設定するには、**config logging syslog facility** コマンドを使用します。

config logging syslog facility *facility_code*

構文の説明	*facility_code*

ファシリティ コード。次のいずれかを選択します。

- authorization：認証システム。ファシリティ レベル：4。
- auth-private：認証システム（プライベート）。ファシリティ レベル：10。
- cron：ファシリティあたりの Cron。ファシリティ レベル：9。
- daemon：システム デーモン。ファシリティ レベル：3。
- ftp：FTP デーモン。ファシリティ レベル：11。
- kern：カーネル。ファシリティ レベル：0。
- local0：ローカル用。ファシリティ レベル：16。
- local1：ローカル用。ファシリティ レベル：17。
- local2：ローカル用。ファシリティ レベル：18。
- local3：ローカル用。ファシリティ レベル：19。
- local4：ローカル用。ファシリティ レベル：20。
- local5：ローカル用。ファシリティ レベル：21。
- local6：ローカル用。ファシリティ レベル：22。
- local7：ローカル用。ファシリティ レベル：23。
- lpr：ライン プリンタ システム。ファシリティ レベル：6。
- mail：メール システム。ファシリティ レベル：2。
- news：USENET ニュース。ファシリティ レベル：7。

- sys12：システム用。ファシリティ レベル：12。
- sys13：システム用。ファシリティ レベル：13。
- sys14：システム用。ファシリティ レベル：14。
- sys15：システム用。ファシリティ レベル：15。
- syslog：syslog 自体。ファシリティ レベル：5。
- user：ユーザ プロセス。ファシリティ レベル：1。
- uucp：Unix-to-Unix コピー システム。ファシリティ レベル：8。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、発信 syslog メッセージのファシリティを認証に設定する例を示します。

```
(Cisco Controller) > config logging syslog facility authorization
```

関連コマンド

config logging syslog host

config logging syslog level

show logging

config logging syslog facility client

syslog ファシリティを AP に設定するには、**config logging syslog facility client** { **assocfail Dot11** | **associate Dot11** | **authentication** | **authfail Dot11** | **deauthenticate Dot11** | **disassociate Dot11** | **exclude**}{ **enable** | **disable**} コマンドを使用します。

config logging syslog facility *Client*

構文の説明

クライアント	ファシリティ クライアント。次の機能があります。 • assocfail Dot11：クライアントの関連付け失敗 syslog • associate Dot11：クライアントの関連付け syslog • authentication：クライアントの認証成功 syslog • authfail Dot11：クライアントの認証失敗 syslog • deauthenticate Dot11：クライアントの認証解除 syslog • disassociate Dot11：クライアントの関連付け解除 syslog • excluded：クライアントの除外 syslog

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドは、リリース 7.5 以前のリリースで導入されました。

次に、クライアントのファシリティ syslog ファシリティを設定する例を示します。

```
cisco controller config logging syslog facility client
```

関連コマンド

show logging flags client

config logging syslog facility ap

syslog ファシリティを AP に設定するには、 **config logging syslog facility ap**{ **associate** | **disassociate**}{ **enable** | **disable**} コマンドを使用します。

config logging syslog facility *AP*

構文の説明

AP	ファシリティ AP。次の機能があります。 • associate：AP の関連付け syslog • disassociate：AP の関連付け解除 syslog

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドは、リリース 7.5 以前のリリースで導入されました。

次に、AP の syslog ファシリティを設定する例を示します。

```
cisco controller config logging syslog facility ap
```

関連コマンド

show logging flags ap

config logging syslog level

リモート ホストへの syslog メッセージをフィルタするための重大度を設定するには、**config logging syslog level** コマンドを使用します。

config logging syslog level *severity_level*

構文の説明

severity_level	重大度。次のいずれかを選択します。 • 緊急：重大度 0 • アラート：重大度 1 • 重要：重大度 2 • エラー：重大度 3 • 警告：重大度 4 • 通知：重大度 5 • 情報：重大度 6 • デバッグ：重大度 7

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、syslog メッセージの重大度を 3 に設定する例を示します。

```
(Cisco Controller) > config logging syslog level 3
```

関連コマンド

config logging syslog host

config logging syslog facility

show logging

config loginsession close

アクティブなすべての Telnet セッションを閉じるには、**config loginsession close** コマンドを使用します。

config loginsession close {*session_id* | **all**}

構文の説明

session_id	閉じるセッションの ID。
all	すべての Telnet セッションを閉じます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクティブなすべての Telnet セッションを閉じる例を示します。

```
(Cisco Controller) > config loginsession close all
```

関連コマンド

show loginsession

config macfilter

Cisco ワイヤレス LAN コントローラで MAC フィルタ エントリを作成または削除するには、**config macfilter** {*add* | *delete*} コマンドを使用します。

config macfilter {**add** *client_MAC wlan_id* [*interface_name*] [*description*] [*macfilter_IP*] | **delete** *client_MAC*}

構文の説明

add	コントローラで MAC フィルタ エントリを追加します。
delete	コントローラで MAC フィルタ エントリを削除します。
MAC_addr	Client MAC address.
wlan_id	MAC フィルタ エントリをアソシエートする無線 LAN 識別子。値が 0 の場合、エントリをすべての無線 LAN にアソシエートします。
interface_name	（任意）インターフェイスの名前。インターフェイスを指定しない場合は **0** を入力してください。
description	（任意）二重引用符で囲まれた最大 32 文字の、インターフェイスの短い説明。 （注） *macfilterIP* を指定する場合、説明は必須です。
IP Address	（任意）ローカル MAC フィルタ データベースの IPv4 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco ワイヤレス LAN コントローラでクライアントを無線 LAN にローカルに追加するには、**config macfilter add** コマンドを使用します。このフィルタは RADIUS 認証プロセスをバイパスします。

リリース 7.6 と同様に、オプションの *macfilter_IP* は IPv4 アドレスだけをサポートしています。

次に、ワイヤレス LAN ID 1、インターフェイス名 labconnect、およびコントローラの MAC フィルタ IP 10.92.125.51 で MAC フィルタ エントリ 00:E0:77:31:A3:55 を追加する例を示します。

```
(Cisco Controller) > config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect"
10.92.125.51
```

関連コマンド

show macfilter

config macfilter ip-address

config macfilter description

MAC フィルタに説明を追加するには、**config macfilter description** コマンドを使用します。

config macfilter description *MAC addrdescription*

構文の説明

MAC addr	クライアント MAC アドレス
description	（任意）二重引用符で囲まれた説明（最大 32 文字）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC フィルタ 01 という説明を MAC アドレス 11:11:11:11:11:11 に設定する例を示します。

```
(Cisco Controller) > config macfilter description 11:11:11:11:11:11 "MAC Filter 01"
```

関連コマンド

show macfilter

config macfilter interface

MAC フィルタのクライアント インターフェイスを作成するには、**config macfilter interface** コマンドを使用します。

config macfilter interface *MAC_addr interface*

構文の説明

MAC addr	クライアント MAC アドレス
interface	インターフェイス名。値 0 は、名前なしに相当します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアント 11:11:11:11:11:11 で MAC フィルタ インターフェイス Lab01 を設定する例を示します。

```
(Cisco Controller) > config macfilter interface 11:11:11:11:11:11 Lab01
```

関連コマンド

show macfilter

config macfilter ip-address

パッシブ クライアントの IP アドレスを入力するには、**config macfilter ip-address** コマンドを使用します。

config macfilterip-address *MAC_addr IP Address*

構文の説明

MAC_addr	クライアントの MAC アドレス。
IP Address	パッシブ クライアントの IP アドレスを追加します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは IPv4 だけをサポートしています。

次に、パッシブ クライアントの IP アドレスを追加する例を示します。

```
(Cisco Controller) > config macfilter ip-address aa-bb-cc-dd-ee-ff 10.92.125.51
```

関連コマンド

show macfilter

config macfilter mac-delimiter

RADIUS サーバに送信される MAC アドレス の MAC デリミタ（コロン、ハイフン、なし、単一ハイフン）を設定するには、**config macfilter mac-delimiter** コマンドを使用します。

config macfilter mac-delimiter {**none** | **colon** | **hyphen** | **single-hyphen**}

構文の説明

none	デリミタを無効にします（xxxxxxxxxx など）。
colon	デリミタをコロンに設定します（xx:xx:xx:xx:xx:xx など）。
hyphen	デリミタをハイフンに設定します（xx-xx-xx-xx-xx-xx など）。
single-hyphen	デリミタを単一ハイフンに設定します（xxxxxx-xxxxxx など）。

コマンド デフォルト

デフォルトのデリミタは、ハイフンです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、aa:bb:cc:dd:ee:ff 形式で MAC アドレスを RADIUS サーバに送信するようにオペレーティング システムを設定する例を示します。

```
(Cisco Controller) > config macfilter mac-delimiter colon
```

次に、aa-bb-cc-dd-ee-ff 形式で MAC アドレスを RADIUS サーバに送信するようにオペレーティング システムを設定する例を示します。

```
(Cisco Controller) > config macfilter mac-delimiter hyphen
```

次に、aabbccddeeff 形式で MAC アドレスを RADIUS サーバに送信するようにオペレーティング システムを設定する例を示します。

```
(Cisco Controller) > config macfilter mac-delimiter none
```

関連コマンド

show macfilter

config macfilter radius-compat

Cisco ワイヤレス LAN コントローラと選択した RADIUS サーバとの互換性を設定するには、**config macfilter radius-compat** コマンドを使用します。

config macfilter radius-compat {**cisco** | **free** | **other**}

構文の説明

cisco	Cisco ACS 互換性モード（パスワードはサーバの MAC アドレス）を設定します。
free	Free RADIUS サーバ互換性モード（パスワードは非公開）を設定します。
other	他のサーバ動作（パスワードは不要）を設定します。

コマンド デフォルト

other

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは IPv4 だけをサポートしています。

次に、Cisco ACS 互換性モードを「その他」に設定する例を示します。

```
(Cisco Controller) > config macfilter radius-compat other
```

関連コマンド

show macfilter

config macfilter wlan-id

MAC フィルタの無線 LAN ID を変更するには、**config macfilter wlan-id** コマンドを使用します。

config macfilter wlan-id *MAC_addr WLAN_id*

構文の説明

MAC addr	クライアント MAC アドレス
WLAN_id	アソシエートする無線 LAN 識別子。値 0 は使用できません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC フィルタ 11:11:11:11:11:11 のクライアントの無線 LAN ID 2 を変更する例を示します。

```
(Cisco Controller) > config macfilter wlan-id 11:11:11:11:11:11 2
```

関連コマンド

show macfilter

show wlan

config mdns ap

アクセス ポイントでマルチキャスト ドメイン ネーム システム（mDNS）スヌーピングを設定するには、**config mdns ap** コマンドを使用します。

config mdns ap {**enable** {*ap_name* | **all**} [**vlan** *vlan_id*] | **disable** {*ap_name* | **all**} | **vlan** {**add** | **delete**} *vlan ap_name*}

構文の説明

enable	アクセス ポイントで mDNS スヌーピングを有効にします。
ap_name	mDNS スヌーピングを設定する必要があるアクセス ポイントの名前。
all	すべてのアクセス ポイントで mDNS スヌーピングを設定します。
vlan	（任意）アクセス ポイントが mDNS パケットをスヌープして転送する VLAN を設定します。
vlan_id	VLAN 識別番号。
disable	アクセス ポイントで mDNS スヌーピングを無効にします。
add	アクセス ポイントが mDNS パケットをスヌープして Cisco ワイヤレス LAN コントローラ（WLC）に転送する VLAN を追加します。mDNS アクセス ポイントには最大 10 の VLAN を設定できます。
delete	アクセス ポイントが mDNS パケットをスヌープして Cisco WLC に転送する VLAN を削除します。

コマンド デフォルト

mDNS 対応アクセス ポイントは、デフォルトでアクセス VLAN またはネイティブ VLAN をスヌープします。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

アクセス ポイントで mDNS スヌーピングを有効にすると、アクセス ポイントは Cisco WLC に表示されない VLAN 上の有線サービスをスヌープできるようになります。mDNS スヌーピングはローカル モードおよびモニタ モードのアクセス ポイントでのみサポートされています。アクセス ポイントはアクセス モードまたはトランク モードになっている必要があります。アクセス ポイントがトランク モードの場合は、アクセス ポイントが mDNS パケットをスヌープして転送する Cisco WLC で VLAN を設定する必要があります。アクセス ポイントが mDNS ク

エリをスヌープして送信するには、Cisco WLC からネイティブ VLAN も設定する必要があります。また、アクセス ポイントは、ネイティブ VLAN でパケットにタグ付けします。

グローバル mDNS スヌーピングは、mDNS アクセス ポイント スヌーピングに優先されます。

次に、アクセス ポイントで mDNS スヌーピングを有効にし、アクセス ポイントが mDNS パケットをスヌープする必要がある VLAN を設定する例を示します。

```
(Cisco Controller) > config mdns ap enable vlan 1
```

config mdns profile

マルチキャストDNS（mDNS）プロファイルを設定して、プロファイルにサービスを関連付けるには、**config mdns profile** コマンドを使用します。

config mdns profile {**create** | **delete** | **service** {**add** | **delete**} *service _name profile_name*

構文の説明

create	mDNS プロファイルを作成します。
delete	mDNS プロファイルを削除します。プロファイルがインターフェイス グループ、インターフェイス、または WLAN に関連付けられている場合は、エラーが表示されます。
service	mDNS サービスを設定します。
add	mDNS プロファイルに mDNS サービスを追加します。
delete	mDNS プロファイルから mDNS サービスを削除します。
service -name	mDNS サービスの名前。
profile_name	mDNS プロファイルの名前。最大 16 個のプロファイルを作成できます。

コマンド デフォルト

デフォルトでは、コントローラに mDNS プロファイル、デフォルト mdns プロファイルがあります。このデフォルト プロファイルは削除できません。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

新しいプロファイルを作成した後、インターフェイス グループ、インターフェイス、またはWLANにプロファイルをマッピングする必要があります。クライアントはプロファイルに関連付けられたサービスのみのサービス アドバタイズメントを受信します。コントローラはインターフェイス グループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイス プロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。

デフォルトでは、コントローラに mDNS プロファイル、デフォルト mdns プロファイルがあります。このデフォルト プロファイルは削除できません。

次に、mDNS profile1 に Apple TV の mDNS サービスを追加する例を示します。

```
(Cisco Controller) > config mdns profile create profile1 Apple TV
```

関連コマンド

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns query interval

マルチキャスト DNS（mDNS）サービスのクエリ間隔を設定するには、**config mdns query interval** コマンドを使用します。

config mdns query interval *interval_value*

構文の説明

interval_value	設定可能な分単位の mDNS クエリ間隔。クエリ間隔とは、コントローラがマスター サービス データベースで定義されているすべてのサービスに定期的にクエリを送信する頻度です。範囲は 10 ～ 120 です。

コマンド デフォルト

mDNS サービスのデフォルトのクエリ間隔は 15 分です。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

コントローラは、マスター サービス データベースで mDNS サービスが利用できる場合にのみ、このサービスのアドバタイズメントをスヌーピングおよび学習します。mDNS は宛先アドレスとしてマルチキャスト IP アドレス 224.0.0.251 を使用し、UDP 宛先ポートとして 5353 を使用します。

次に、mDNS サービスのクエリ間隔を 20 分間に設定する例を示します。

```
(Cisco Controller) > config mdns query interval 20
```

関連コマンド

config mdns profile

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns service

マスター サービス データベースにマルチキャスト DNS（mDNS）サービスを設定するには、**config mdns service** コマンドを使用します。

次のコマンドは、リリース 7.5 以降のリリースで使用できます。

config mdns service {**create** *service_name service_string* **origin** {**Wireless** | **Wired** | **All**} **lss** {**enable** | **disable**} [**query** {**enable** | **disable**}] | **lss** {**enable** | **disable**} {*service_name* | **all**} | **priority-mac** {**add** | **delete**} *priority-mac service_name* [**ap-group** *ap-group-name*] | **origin** {**Wireless** | **Wired** | **All**} {*service_name* | **all**}}

構文の説明

create	マスターサービスデータベースに新しいmDNSサービスを追加します。
service_name	mDNS サービスの名前。たとえば、Air Tunes、iTunes Music Sharing、FTP、Apple File Sharing Protocol（AFP）などです。
service_string	mDNS サービスに関連付けられた一意の文字列。たとえば、_airplay._tcp.local. は、AppleTV に関連付けられたサービス文字列です。
delete	マスターサービスデータベースからmDNSサービスを削除します。サービスを削除する前に、コントローラはプロファイルがサービスを使用しているかどうかを確認します。 （注） サービスを削除する前に、すべてのプロファイルからサービスを削除する必要があります。
query	mDNS サービスのクエリー ステータスを設定します。
enable	コントローラによる mDNS サービスの定期クエリーをイネーブルにします。
disable	コントローラによる mDNS サービスの定期クエリーをディセーブルにします。
origin	mDNS サービスの発信元を設定します。サービスの発信元を有線またはワイヤレスに制限できます。
Wireless	mDNS サービスの発信元をワイヤレスとして設定します。
Wired	mDNS サービスの発信元を有線として設定します。
All	mDNS サービスの発信元をワイヤレスまたは有線として設定します。

lss	1 つのサービスまたはすべての mDNS サービスのロケーション固有サービス（LSS）を設定します。LSS は登録済みのサービス プロバイダーには適用されません。クエリ元クライアントがユーザと一致する場合は、登録済みのサービス プロバイダーが常に含まれます。有線のみに設定されたサービスについては LSS を設定できません。
all	すべての mDNS サービスの LSS を設定します。
priority-mac	サービス プロバイダー デバイスの MAC アドレスを設定します。このデバイスは、サービス プロバイダー データベースがいっぱいであっても優先されます。
add	優先されるサービス プロバイダー デバイスの MAC アドレスを追加します。 1 つのサービスについて最大 50 の MAC アドレスを設定できます。
delete	優先リストからサービス プロバイダー デバイスの MAC アドレスを削除します。
priority-mac	優先する必要があるサービス プロバイダー デバイスの MAC アドレス。MAC アドレスはサービスごとに一意である必要があります。
ap-group	有線サービス プロバイダーのアクセス ポイント グループを設定します。これらのサービス プロバイダーは他のサービス プロバイダーよりも優先されます。クライアントの mDNS クエリがこの AP グループから発信されると、優先 MAC アドレスを持つ有線エントリとアクセス ポイント グループのリストが集約応答の最初に示されます。
ap-group-name	サービス プロバイダーが属するアクセス ポイント グループの名前。

コマンド デフォルト

デフォルトでは、LSS は無効になっていますが、検出されるすべてのサービスに関して有効になります。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。
7.5	このコマンドが変更されました。**origin**、**Wireless**、**Wired**、**All**、**lss**、**priority-mac**、**add**、**delete**、**ap-group** キーワードと *priority-mac ap-group-name* 引数が追加されました。

使用上のガイドライン

リリース7.5以降のリリースでは、各コントローラ モデルのサービス プロバイダーの最大数は次のとおりです。

- Cisco 5500 シリーズ コントローラと Cisco 2500 シリーズ コントローラ：6400
- Cisco ワイヤレス サービス モジュール 2：6400
- Cisco 8500 シリーズ コントローラと Cisco 7500 シリーズ コントローラ：16000

サービスのLSSが有効になっている場合、発信元がワイヤレスに設定されているサービスを有線に変更できません。

次に、HTTP mDNS サービスをマスター サービス データベースに追加して、発信元をワイヤレスに設定し、そのサービスの LSS を有効にする例を示します。

```
(Cisco Controller) > config mdns service create http _http._tcp.local. origin wireless
lss enable
```

次に、HTTP サービス プロバイダー デバイスの優先 MAC アドレスを追加する例を示します。

```
(Cisco Controller) >config mdns service priority-mac add 44:03:a7:a3:04:45 http
```

config mdns snooping

Cisco WLC でグローバル マルチキャスト DNS（mDNS）スヌーピングを有効または無効にするには、**config mdns snooping** コマンドを使用します。

config mdns snooping {**enable** | **disable**}

構文の説明

enable	Cisco WLC でグローバル mDNS スヌーピングを有効にします。
disable	Cisco WLC でグローバル mDNS スヌーピングを無効にします。

コマンド デフォルト

デフォルトでは、Cisco WLC で mDNS スヌーピングが有効になっています。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

mDNS サービス検出では、ローカル ネットワーク上のサービスをアナウンスし、検出するための手段を提供します。mDNS は、IP マルチキャストで DNS クエリを実行します。mDNS はゼロ コンフィギュレーション IP ネットワーキングをサポートします。

次に、IGMP スヌーピングを有効にする例を示します。

```
(Cisco Controller) > config mdns snooping enable
```

関連コマンド

config mdns query interval

config mdns service

config mdns profile

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config mdns policy enable

mDNS ポリシーを設定するには、**config mdns policy enable | disable** コマンドを使用します。

config mdnspolicyenable | disable

構文の説明

policy	mDNS ポリシーの名前。
enable	コントローラによる mDNS サービスのポリシーを有効にします。
disable	コントローラによる mDNS サービスのポリシーを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは 8.0 リリース以降で使用できます。

例

次に、mDNS ポリシーを設定する例を示します。

```
(Cisco Controller) >config mdns
  policy enable
```

config mdns policy service-group

mDNS ポリシー サービス グループを作成または削除するには、**config mdns policy service-group** コマンドを使用します。

config mdns policy service-group {**create** | **delete**} *service-group-name*

構文の説明

create	mDNS サービス グループを作成します。
delete	mDNS サービス グループを削除します。
service-group-name	サービス グループの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、mDNS サービス グループを削除する例を示します。

```
(Cisco Controller) >config mdns policy service-group create <service-group-name>
```

config mdns policy service-group parameters

サービス グループのパラメータを設定するには、 **config mdns policy service-group** コマンドを使用します。

config mdnspolicyservice-group device-mac add *service-group-name mac-addr device name* **location-type** *[AP_LOCATION | AP_NAME |AP_GROUP]* **device-location** *[location string |any | same]*

構文の説明

device-mac	サービス プロバイダー デバイスの MAC アドレスを設定します。
add	サービスプロバイダーデバイスのサービス グループ名を追加します。
service-group-name	mDNS サービス グループの名前。
device-name	サービス プロバイダーが属しているデバイスの名前。
location type	サービスプロバイダーデバイスのロケーション タイプを設定します。
[AP_LOCATION | AP_NAME | AP_GROUP]	アクセス ポイントの名前、位置、グループ。
device-location	サービス プロバイダーが属しているデバイスの位置を設定します。
[location string |any | same]	デバイスの位置を表す文字列。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、サービス プロバイダー デバイスのロケーション タイプを設定する例を示します。

```
(Cisco Controller) >config mdns policy service-group location type [AP_LOCATION | AP_NAME
 | AP_GROUP]
```

config mdns policy service-group user-name

mDNS サービス グループのユーザ ロールを設定するには、**config mdns policy service-group user-name add | delete <service-group-name> <user-role-name>** コマンドを使用します。

config mdnspolicyservice-groupuser-nameadd | delete*service-group-name user-name*

構文の説明

user-name	mDNS サービス グループのユーザの名前を設定します。
service-group-name	mDNS サービス グループの名前。
user-name	mDNS サービス グループのユーザ ロールの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、mDNS サービス グループのユーザ名を追加する例を示します。

```
(Cisco Controller) >config mdns policy service-group user-name add <service-group-name>
 <user-role-name>
```

config mdns policy service-group user-role

mDNS サービス グループのユーザ ロールを設定するには、**config mdns policy service-group user-role add | delete <service-group-name> <user-role-name>** コマンドを使用します。

config mdnspolicyservice-groupuser-roleadd | delete*service-group-name user-role-name*

構文の説明

user-role	mDNS サービス グループのユーザ ロールを設定します。
service-group-name	mDNS サービス グループの名前。
user-role-name	mDNS サービス グループのユーザ ロールの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

例

次に、mDNS サービス グループのユーザ ロール詳細情報を追加する例を示します。

```
(Cisco Controller) >config mdns policy service-group user-role add <service-group-name>
 <user-role-name>
```

config media-stream multicast-direct

メディア ストリーム マルチキャスト ダイレクトを設定するには、**config media-stream multicast direct** コマンドを使用します。

config media-stream multicast-direct {**enable** | **disable**}

構文の説明

enable	メディア ストリームを有効にします。
disable	メディア ストリームを無効にします。

コマンド デフォルト

なし。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

次に、メディア ストリーム マルチキャスト ダイレクト設定を有効にする例を示します。

```
> config media-stream multicast-direct enable
```

次に、メディア ストリーム マルチキャスト ダイレクト設定を無効にする例を示します。

```
> config media-stream multicast-direct disable
```

関連コマンド

config 802.11 media-stream video-redirect

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream message

メッセージ設定のさまざまなパラメータを設定するには、**config media-stream message** コマンドを使用します。

config media-stream message {**state**［**enable** | **disable**］ | **url** *url* | **email** *email* | **phone** *phone_number* | **note** *note*}

構文の説明

state	メディア ストリーム メッセージの状態を指定します。
enable	（任意）セッション アナウンス メッセージの状態を有効にします。
disable	（任意）セッション アナウンス メッセージの状態を無効にします。
url	URL を設定します。
url	セッション アナウンス URL。
email	電子メール ID を設定します。
email	セッション アナウンスの電子メールを指定します。
phone	電話番号を設定します。
phone_number	セッション アナウンスの電話番号。
note	メモを設定します。
note	セッション アナウンスのメモ。

コマンド デフォルト

ディセーブル

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

次に、セッション アナウンスメント メッセージの状態を有効にする例を示します。

```
> config media-stream message state enable
```

次に、セッション アナウンスの電子メール アドレスを設定する例を示します。

```
> config media-stream message mail abc@co.com
```

関連コマンド

config media-stream

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream add

さまざまなグローバル メディア ストリーム設定を行うには、**config media-stream add** コマンドを使用します。

config media-stream add multicast-direct *media_stream_name start-IP end-IP* [**template** {**very coarse** | **coarse** | **ordinary** | **low-resolution** | **med-resolution** | **high-resolution**} | **detail** {*bandwidth packet-size* {**periodic** | **initial**}} **qos** *priority* {**drop** | **fallback**}

構文の説明

multicast-direct	マルチキャスト ダイレクト設定のメディア ストリームを指定します。
media_stream_name	メディア ストリームの名前。
start-IP	IP マルチキャストの宛先開始アドレス。
end-IP	IP マルチキャストの宛先終了アドレス。
template	（任意）テンプレートからのメディア ストリームを設定します。
very coarse	非常に粗いテンプレートを適用します。
coarse	粗いテンプレートを適用します。
ordinary	通常のテンプレートを適用します。
low-resolution	低解像度のテンプレートを適用します。
med-resolution	通常の解像度のテンプレートを適用します。
high-resolution	高解像度のテンプレートを適用します。
detail	特定のパラメータでメディア ストリームを設定します。
bandwidth	予想される最大ストリーム帯域幅。
packet-size	平均パケット サイズ。
periodic	定期的なアドミッション評価を指定します。
initial	最初のアドミッション評価を指定します。
qos	AIR QoS クラス（ビデオのみ）。
priority	メディア ストリームの優先順位。
drop	ストリームが定期的な再評価でドロップされるように指定します。

fallback	定期的な再評価でストリームがベストエフォートクラスに降格されるかどうかを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

次に、新しいメディア ストリームを設定する例を示します。

```
> config media-stream add multicast-direct abc 227.8.8.8 227.9.9.9 detail 2 150 periodic
 video 1 drop
```

関連コマンド

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream admit

メディア ストリーム グループのトラフィックを許可するには、**config media-stream admit** コマンドを使用します。

config media-stream admit *media_stream_name*

構文の説明

media_stream_name	メディア ストリームのグループ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディアストリーム グループのトラフィックを許可しようとすると、IGMP スヌーピングを無効にして再度有効にすることを求めるプロンプトが表示されます。また、マルチキャスト トラフィックの異常がすべてのクライアントに対して発生する場合があります。

次に、メディア ストリーム グループのトラフィックを許可する例を示します。

```
(Cisco Controller) > config media-stream admit MymediaStream
```

関連コマンド

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream deny

メディア ストリーム グループのトラフィックをブロックするには、**config media-stream deny** コマンドを使用します。

構文の説明

media_stream_name	メディア ストリームのグループ名。

config media-stream deny *media_stream_name*

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

メディアストリーム グループのトラフィックをブロックしようとすると、IGMP スヌーピングを無効にして再度有効にすることを求めるプロンプトが表示されます。また、マルチキャストトラフィックの異常がすべてのクライアントに対して発生する場合があります。

次に、メディア ストリーム グループのトラフィックをブロックする例を示します。

```
(Cisco Controller) > config media-stream deny MymediaStream
```

関連コマンド

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream delete

さまざまなグローバル メディア ストリーム設定を行うには、**config media-stream delete** コマンドを使用します。

config media-stream delete *media_stream_name*

構文の説明

media_stream_name	メディア ストリームの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

次に、abc という名前のメディア ストリームを削除する例を示します。

```
(Cisco Controller) > config media-stream delete abc
```

関連コマンド

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config memory monitor errors

メモリ エラーおよびメモリ リークのモニタリングを有効または無効にするには、**config memory monitor errors** コマンドを使用します。

config memory monitor errors {**enable** | **disable**}

⚠

注意 **config memory monitor** コマンドはシステムに悪影響を及ぼす可能性があるので、Cisco TAC の指示を受けた場合に限り実行する必要があります。

構文の説明

enable	メモリ設定のモニタリングをイネーブルにします。
disable	メモリ設定のモニタリングをディセーブルにします。

コマンド デフォルト

メモリ エラーおよびリークのモニタリングは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

操作について知識があり、問題が検出され、トラブルシューティング情報の収集が行われている場合を除き、**config memory monitor** コマンドのデフォルトの変更は慎重に行うようにしてください。

次に、コントローラのメモリ エラーおよびリークのモニタリングを有効にする例を示します。

```
(Cisco Controller) > config memory monitor errors enable
```

関連コマンド

config memory monitor leaks

debug memory

show memory monitor

config memory monitor leaks

2 つのメモリしきい値の間で自動リーク分析を実行するようにコントローラを設定するには、**config memory monitor leaks** コマンドを使用します。

config memory monitor leaks *low_thresh high_thresh*

注意 **config memory monitor** コマンドはシステムに悪影響を及ぼす可能性があるので、Cisco TAC の指示を受けた場合に限り実行する必要があります。

構文の説明

low_thresh	空きメモリがクラッシュする下限値。この値は 10,000 KB 未満に設定できません。
high_thresh	コントローラが auto-leak-analysis モードになる下限値。「使用上のガイドライン」の項を参照してください。

コマンド デフォルト

low_thresh のデフォルト値は 10000 KB であり、*high_thresh* のデフォルト値は 30000 KB です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

（注） 操作について知識があり、問題が検出され、トラブルシューティング情報の収集が行われている場合を除き、**config memory monitor** コマンドのデフォルトの変更は慎重に行うようにしてください。

メモリ リークのおそれがある場合は、このコマンドを使用します。

空きメモリが *low_thresh* しきい値を下回ると、システムがクラッシュしてクラッシュ ファイルが生成されます。このパラメータのデフォルト値は 10,000 KB です。この値より低い値に設定できません。

high_thresh しきい値は、現在の空きメモリの大きさ以上に設定してください。このようにすると、システムは自動リーク分析モードになります。空きメモリの大きさが、指定された *high_thresh* しきい値を下回ると、メモリ割り当てのトラッキングと解放のプロセスが開始します。その結果、**debug memory events enable** コマンドによってすべての割り当てと空きメモリが表示され、 **show memory monitor detail** コマンドによってメモリ リークの疑いの検出が開始されます。

次に、auto-leak-analysis モードのしきい値を、下限しきい値 12000 KB と上限しきい値 35000 KB に設定する例を示します。

```
(Cisco Controller) > config memory monitor leaks 12000 35000
```

関連コマンド

config memory monitor leaks

debug memory

show memory monitor

config mesh alarm

屋外メッシュ アクセス ポイントのアラーム設定を行うには、**config mesh alarm** コマンドを使用します。

config mesh alarm {**max-hop** | **max-children** | **low-snr** | **high-snr** | **association** | **parent-change count**} *value*

構文の説明

max-hop	メッシュ ネットワーク上のトラフィックでアラームをトリガーするまでの最大ホップ カウントを設定します。有効な値は 1 ～ 16 です。
max-children	メッシュルートアクセスポイント（RAP）に割り当てることのできるメッシュアクセスポイント（MAP）の最大数を設定します。この数を超えると、アラームがトリガーされます。有効な値は 1 ～ 16 です。
low-snr	信号対雑音比（SNR）の下限値を設定します。この値を下回ると、アラームがトリガーされます。有効な値は 1 ～ 30 です。
high-snr	SNR の上限値を設定します。この値を超えると、アラームがトリガーされます。有効な値は 1 ～ 30 です。
association	メッシュ アラームのアソシエーション数値を設定します。この値を超えると、アラームがトリガーされます。有効な値は 1 ～ 30 です。
parent-change count	MAP で RAP アソシエーションを変更できる回数を設定します。この回数を超えると、アラームがトリガーされます。有効な値は 1 ～ 30 です。
value	この値を上回る、または下回るとアラームが生成される、トリガー値。有効な値は、コマンドごとに異なります。

コマンド デフォルト

コマンドおよび引数の値の範囲については、「構文の説明」の項を参照してください。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、最大ホップのしきい値を 8 に設定する例を示します。

```
(Cisco Controller) >config mesh alarm max-hop 8
```

次に、SNR の上限しきい値を 25 に設定する例を示します。

```
(Cisco Controller) >config mesh alarm high-snr 25
```

config mesh astools

屋外メッシュ アクセス ポイントの孤立防止機能をグローバルに有効または無効にするには、**config mesh astools** コマンドを使用します。

config mesh astools {**enable** | **disable**}

構文の説明

enable	すべての屋外メッシュ アクセス ポイントに対してこの機能を有効にします。
disable	すべての屋外メッシュ アクセス ポイントに対してこの機能を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての屋外メッシュ アクセス ポイントの孤立防止機能を有効にする例を示します。

```
(Cisco Controller) >config mesh astools enable
```

config mesh backhaul rate-adapt

屋内および屋外メッシュ アクセス ポイントに対してバックホール送信レート適応（ユニバーサル アクセス）をグローバルに設定するには、**config mesh backhaul rate-adapt** コマンドを使用します。

config mesh backhaul rate-adapt ［**all** | **bronze** | **silver** | **gold** | **platinum**］｛**enable** | **disable**｝

構文の説明

all	（任意）メッシュ アクセス ポイントでユニバーサル アクセス権限を許可します。
bronze	（任意）メッシュ アクセス ポイントでバックグラウンド レベルのクライアント アクセス権限が許可されます。
silver	（任意）メッシュ アクセス ポイントでベストエフォート レベルのクライアント アクセス権限が許可されます。
gold	（任意）メッシュ アクセス ポイントでビデオ レベルのクライアント アクセス権限が許可されます。
platinum	（任意）メッシュ アクセス ポイントで音声レベルのクライアント アクセス権限が許可されます。
enable	メッシュ アクセス ポイントのこのバックホール アクセス レベルを有効にします。
disable	メッシュ アクセス ポイントのこのバックホール アクセス レベルを無効にします。

コマンド デフォルト

メッシュ アクセス ポイントのバックホール アクセス レベルは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用するには、クライアント アクセスを持つメッシュ バックホールを **config mesh client-access** コマンドを使用して有効にする必要があります。

（注） この機能をイネーブルにすると、すべてのメッシュ アクセス ポイントがリブートします。

次にバックホール クライアント アクセスをベストエフォート レベルに設定する例を示します。

```
(Cisco Controller) >config mesh backhaul rate-adapt silver
```

config mesh backhaul slot

ダウンリンクのバックホールとしてスロットの無線を設定するには、**config mesh backhaul slot** コマンドを使用します。

config mesh backhaul slot *slot_id* {**enable** | **disable**} *cisco_ap*

構文の説明

slot_id	0～2 の間のスロット番号。
enable	ダウンリンクのバックホールとして入力されたスロットの無線を有効にします。
disable	ダウンリンクのバックホールとして入力されたスロットの無線を無効にします。
cisco_ap	バックホールを有効にするか、無効にする必要があるセクターのルート AP の名前。

コマンド デフォルト

ダウンリンクのバックホールとして入力されたスロットの無線は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

2.4 GHz の場合、スロット 0 と 1 のみが有効です。スロット 0 が有効になっている場合、スロット 1 が自動的に無効になります。スロット 0 が無効になっている場合、スロット 1 が自動的に有効になります。

次に、ルート AP myrootap1 の優先バックホールとしてスロット 1 を有効にする例を示します。

```
(Cisco Controller) >config mesh backhaul slot 1 enable myrootap1
```

config mesh battery-state

Cisco Aironet 1520 シリーズのメッシュ アクセス ポイントのバッテリ状態を設定するには、**config mesh battery-state** コマンドを使用します。

config mesh battery-state {**enable** | **disable**} {**all** | *cisco_ap* }

構文の説明

enable	1520 シリーズのメッシュ アクセス ポイントのバッテリ状態を有効にします。
disable	1520 シリーズのメッシュ アクセス ポイントのバッテリ状態を無効にします。
all	すべてのメッシュ アクセス ポイントにこのコマンドを適用します。
cisco_ap	特定のメッシュ アクセス ポイント。

コマンド デフォルト

バッテリ状態は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次にバックホール クライアント アクセスをベストエフォート レベルに設定する例を示します。

```
(Cisco Controller) >config mesh battery-state enable all
```

config mesh client-access

屋内または屋外のメッシュ アクセス ポイントでメッシュ バックホールへのクライアント アクセスを有効または無効にするには、**config mesh client-access** コマンドを使用します。

config mesh client-access {**enable** [**extended**] | **disable**}

構文の説明

enable	メッシュ アクセス ポイントのバックホール 802.11a 無線経由での無線クライアント アソシエーションを許可します。
extended	（任意）バックホール アクセス ポイントに対する両方のバックホール無線上でクライアント アクセスを有効にします。
disable	802.11a 無線をバックホール トラフィックに制限し、802.11b/g 無線経由でのクライアント アソシエーションだけを許可します。

コマンド デフォルト

クライアント アクセスは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

バックホール インターフェイス（802.11a 無線）は、プライマリ イーサネット インターフェイスとして機能します。バックホールはネットワーク内のトランクとして機能し、無線ネットワークと有線ネットワークとの間のすべての VLAN トラフィックを伝送します。プライマリ イーサネット インターフェイスに必要な設定はありません。

この機能が有効の場合、メッシュ アクセス ポイントで、802.11a 無線上で無線クライアント アソシエーションを許可します。つまり、152x メッシュ アクセス ポイントは、同一の 802.11a 無線経由でバックホール トラフィックと 802.11a クライアント トラフィックの両方を伝送できます。

この機能を無効にすると、メッシュ アクセス ポイントでは、802.11a 無線でバックホール トラフィックが伝送され、クライアント アソシエーションは 802.11b/g 無線のみで行われます。

次に、802.11a 無線上で無線クライアント アソシエーションを許可するために拡張されたクライアント アクセスを有効にする例を示します。

```
(Cisco Controller) >config mesh client-access enable extended
Enabling client access on both backhaul slots
 Same BSSIDs will be used on both slots
 All Mesh AP will be rebooted
 Are you sure you want to start? (y/N)Y
```

次に、無線クライアント アソシエーションを 802.11b/g 無線に制限する例を示します。

```
(Cisco Controller) >config mesh client-access disable
All Mesh AP will be rebooted
Are you sure you want to start? (Y/N) Y
Backhaul with client access is canceled.
```

config mesh convergence

すべてのメッシュ アクセス ポイントでメッシュ コンバージェンス方式を設定するには、**config mesh convergence** コマンドを使用します。

config mesh convergence {**fast** [**standard**] | **very-fast**} *all*

構文の説明

fast	高速コンバージェンス方式を設定します。
standard	標準コンバージェンス方式を設定します。
very-fast	超高速コンバージェンス方式を設定します。
all	選択したメッシュ コンバージェンス方式をすべてのメッシュ アクセス ポイントで設定します。

コマンド デフォルト

デフォルトのメッシュ コンバージェンス方式は標準です。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

標準コンバージェンス方式は、リリース 7.6 以降で使用できます。高速および超高速コンバージェンス方式は、リリース 8.0 以降で使用できます。

次の表は各種コンバージェンス方式を示します。

コンバージェンス方式	親損失のタイマー（秒単位）。	チャンネルごとの検索のタイマー（秒単位）。	親、ネイバー キープアライブのタイマー（秒単位）。
Standard	21	3	3
Fast	7	2	3
Very Fast	4	2	1.5

次に、メッシュ コンバージェンスを Standard に設定する例を示します。

```
(Cisco Controller) >config mesh convergence standard all
```

config mesh ethernet-bridging allow-bpdu

有線メッシュ アップリンクへの STP BPDU を設定するには、**config mesh ethernet-bridging allow-bpdu** コマンドを使用します。

config mesh ethernet-bridging allow-bpdu {**enable** | **disable**}

構文の説明

enable	有線メッシュ アップリンクへの STP BPDU を有効にします。
disable	有線メッシュ アップリンクへの STP BPDU を無効にします。

コマンド デフォルト

無効

コマンド履歴

リリース	変更内容
8.0.110.0	このコマンドが導入されました。

使用上のガイドライン

VLAN 透過性が有効になっている場合、Cisco WLC ではこのコマンドを使用できません。

config mesh ethernet-bridging vlan-transparent

メッシュ アクセス ポイントでイーサネット ブリッジド トラフィックの VLAN タグを処理する方法を設定するには、**config mesh ethernet-bridging vlan-transparent** コマンドを使用します。

config mesh ethernet-bridging vlan-transparent {**enable** | **disable**}

構文の説明

enable	パケットをタグなしであるかのようにブリッジします。
disable	すべてのタグ付きパケットをドロップします。

コマンド デフォルト

パケットをタグなしであるかのようにブリッジします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、イーサネット パケットをタグなしとして設定する例を示します。

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent enable
```

次に、タグ付きイーサネット パケットをドロップする例を示します。

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent disable
```

config mesh full-sector-dfs

メッシュ アクセス ポイントでフルセクタの動的周波数選択（DFS）をグローバルに有効または無効にするには、**config mesh full-sector-dfs** コマンドを使用します。

config mesh full-sector-dfs {**enable** | **disable**}

構文の説明

enable	メッシュ アクセス ポイントの DFS を有効にします。
disable	メッシュ アクセス ポイントの DFS を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、レーダー信号の検出時にチャネル変更の調整を行うようにメッシュセクターに指示します。たとえば、メッシュアクセスポイント（MAP）がレーダー信号を検出すると、MAP はルート アクセス ポイント（RAP）に通知し、RAP はセクター変更を開始します。

このセクターに属するすべての MAP および RAP は新しいチャネルに移動します。これにより、現在のバックホールチャネルでレーダーが検出され、バックアップとして使用可能な他の有効な親が存在しない場合に、MAP が孤立する可能性を低減します。

各セクターの変更により、（DFS 標準で定められているように）ネットワークが 60 秒間応答を停止します。

30 分後には、RAP は以前に設定されたチャネルに戻ります。これは、RAP のチャネルでレーダーが頻繁に検出される場合、この RAP に別のチャネルを設定し、コントローラでレーダーの影響を受けたチャネルを除外することが重要であることを意味します。

次に、メッシュ アクセス ポイントでフルセクタの DFS を有効にする例を示します。

```
(Cisco Controller) >config mesh full-sector-dfs enable
```

config mesh linkdata

アクセス ポイントの外部 MAC フィルタリングを有効にするには、**config mesh linkdata** コマンドを使用します。

config mesh linkdata *destination_ap_name*

構文の説明

destination_ap_name	MACアドレス フィルタリングの宛先アクセス ポイント名。

コマンド デフォルト

外部 MAC フィルタリングは無効になっています。

使用上のガイドライン

（注） **config mesh linktest** コマンドと **config mesh linkdata** コマンドは、同時に使用して、発信元アクセス ポイントと宛先アクセス ポイントで情報を照合するように設計されています。この情報を取得するには、まず *dest_ap* 引数でデータのリンク元になるアクセス ポイントを指定して **config mesh linktest** コマンドを実行します。このコマンドが完了して、同じ宛先アクセス ポイントをリスト表示する **config mesh linkdata** コマンドを実行すると、リンク データが表示されます（例を参照）。

デフォルトでは、MAC フィルタリングは、コントローラ上のローカル MAC フィルタを使用します。

外部 MAC フィルタ認証が有効であり、MAC アドレスがローカル MAC フィルタで検出されない場合には、外部 RADIUS サーバの MAC アドレスが使用されます。

MAC フィルタリングにより、外部サーバで定義されていないアクセスポイントの参加を防止して、不正なメッシュ アクセス ポイントからネットワークを保護します。

メッシュ ネットワーク内で外部認証を利用するには、次の設定が必要です。

- AAA サーバとして使用する RADUIS サーバをコントローラで設定する必要があります。
- コントローラも、RADIUS サーバで設定する必要があります。
- 外部認証および認証用に設定されたメッシュ アクセス ポイントは、RADIUS サーバのユーザ リストに追加する必要があります。

次に、アクセス ポイント AP001d.710d.e300 での外部 MAC アドレス フィルタリングを有効にする例を示します。

```
(Cisco Controller) >config mesh linkdata MAP2-1-1522.7400 AP001d.710d.e300 18 100 1000
30
LinkTest started on source AP, test ID: 0
[00:1D:71:0E:74:00]->[00:1D:71:0D:E3:0F]
Test config:  1000 byte packets at 100  pps for 30 seconds, a-link rate 18 Mb/s
In progress: | || || || || || || || || || || || |
```

```
LinkTest complete
Results
=======
txPkts:             2977
txBuffAllocErr:        0
txQFullErrs:           0
Total rx pkts heard at destination:      2977
rx pkts decoded correctly:               2977
  err pkts: Total         0 (PHY 0 + CRC 0 + Unknown 0), TooBig 0, TooSmall 0
  rx lost packets:        0 (incr for each pkt seq missed or out of order)
  rx dup pkts:            0
  rx out of order:        0
avgSNR:    30, high:   33, low:    3
SNR profile         [0dB...60dB]
          0            6            0            0            0
          0            0            1            2           77
       2888            3            0            0            0
          0            0            0            0            0
    (>60dB)            0
avgNf:    -95, high:  -67, low:  -97
Noise Floor profile [-100dB...-40dB]
          0         2948           19            3            1
          0            0            0            0            0
          3            3            0            0            0
          0            0            0            0            0
    (>-40dB)           0
avgRssi:   64, high:   68, low:   63
RSSI profile        [-100dB...-40dB]
          0            0            0            0            0
          0            0            0            0            0
          0            0            0            0            0
          0            0            0            0            0
    (>-40dB)        2977
Summary PktFailedRate (Total pkts sent/recvd):                        0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%
```

次に、アクセス ポイント AP001d.71d.e300 の外部 MAC フィルタリングを有効にする例を示します。

```
(Cisco Controller) >config mesh linkdata AP001d.710d.e300
[SD:0,0,0(0,0,0), 0,0, 0,0]
[SD:1,105,0(0,0,0),30,704,95,707]
[SD:2,103,0(0,0,0),30,46,95,25]
[SD:3,105,0(0,0,0),30,73,95,29]
[SD:4,82,0(0,0,0),30,39,95,24]
[SD:5,82,0(0,0,0),30,60,95,26]
[SD:6,105,0(0,0,0),30,47,95,23]
[SD:7,103,0(0,0,0),30,51,95,24]
[SD:8,105,0(0,0,0),30,55,95,24]
[SD:9,103,0(0,0,0),30,740,95,749]
[SD:10,105,0(0,0,0),30,39,95,20]
[SD:11,104,0(0,0,0),30,58,95,23]
[SD:12,105,0(0,0,0),30,53,95,24]
[SD:13,103,0(0,0,0),30,64,95,43]
[SD:14,105,0(0,0,0),30,54,95,27]
[SD:15,103,0(0,0,0),31,51,95,24]
[SD:16,105,0(0,0,0),30,59,95,23]
[SD:17,104,0(0,0,0),30,53,95,25]
[SD:18,105,0(0,0,0),30,773,95,777]
[SD:19,103,0(0,0,0),30,745,95,736]
[SD:20,105,0(0,0,0),30,64,95,54]
[SD:21,103,0(0,0,0),30,747,95,751]
[SD:22,105,0(0,0,0),30,55,95,25]
```

```
[SD:23,104,0(0,0,0),30,52,95,35]
[SD:24,105,0(0,0,0),30,134,95,23]
[SD:25,103,0(0,0,0),30,110,95,76]
[SD:26,105,0(0,0,0),30,791,95,788]
[SD:27,103,0(0,0,0),30,53,95,23]
[SD:28,105,0(0,0,0),30,128,95,25]
[SD:29,104,0(0,0,0),30,49,95,24]
[SD:30,0,0(0,0,0), 0,0, 0,0]
```

config mesh linktest

メッシュ アクセス ポイント間のクライアント アクセスを確認するには、**config mesh linktest** コマンドを使用します。

config mesh linktest *source_ap* {*dest_ap* | *MAC addr*} *datarate packet_rate packet_size duration*

構文の説明

source_ap	発信元アクセス ポイント。
dest_ap	宛先アクセス ポイント。
MAC addr	MAC アドレス。
datarate	• 802.11a 無線のデータ レート。有効な値は 6、9、11、12、18、24、36、48、54 Mbps です。 • 802.11b 無線のデータ レート。有効な値は、6、12、18、24、36、54、100 Mbps です。 • 802.11n 無線のデータ レート。有効な値は m0 ～ m15 間の MCS レートです。
packet_rate	パケット数/秒。有効な範囲は 1 ～ 3000 ですが、推奨されるデフォルトは 100 です。
packet_size	（任意）バイト単位のパケット サイズ。指定されていない場合、パケット サイズは 1500 バイトにデフォルト設定されます。
duration	（任意）秒単位のテスト期間。有効な値は、10 ～ 300 秒です。指定されていない場合、期間は 30 秒にデフォルト設定されます。

コマンド デフォルト

100 パケット/秒、1500 バイト、30 秒間。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config mesh linktest コマンドと **config mesh linkdata** コマンドは、同時に使用して、発信元アクセス ポイントと宛先アクセス ポイントで情報を照合するように設計されています。この情報を取得するには、まず *dest_ap* 引数でデータのリンク元になるアクセス ポイントを指定して **config mesh linktest** コマンドを入力します。このコマンドが完了して、**config mesh linkdata** コ

マンドを入力すると、同じ宛先アクセス ポイントがリスト表示され、リンク データが表示されます。

リンクをオーバーサブスクライブするおそれのあるリンクテストを実行すると、次の警告メッセージが表示されます。

```
Warning! Data Rate (100 Mbps) is not enough to perform this link test
on packet size (2000bytes) and (1000) packets per second. This may cause
AP to disconnect or reboot. Are you sure you want to continue?
```

次に、メッシュ アクセス ポイント *SB_MAP1* と *SB_RAP2*（*36 Mbps*、*20 fps*、*100* フレーム サイズ、*15* 秒間）のクライアント アクセスを確認する例を示します。

```
(Cisco Controller) >config mesh linktest SB_MAP1 SB_RAP1 36 20 100 15
LinkTest started on source AP, test ID: 0
[00:1D:71:0E:85:00]->[00:1D:71:0E:D0:0F]
Test config:  100 byte packets at 20  pps for 15 seconds, a-link rate 36 Mb/s
In progress: | || || || || || |
LinkTest complete
Results
=======
txPkts:              290
txBuffAllocErr:        0
txQFullErrs:           0
Total rx pkts heard at destination:       290
rx pkts decoded correctly:
  err pkts: Total         0 (PHY 0 + CRC 0 + Unknown 0), TooBig 0, TooSmall 0
  rx lost packets:        0 (incr for each pkt seq missed or out of order)
  rx dup pkts:            0
  rx out of order:        0
avgSNR:    37, high:   40, low:    5
SNR profile         [0dB...60dB]
          0            1            0            0            1
          3            0            1            0            2
          8           27          243            4            0
          0            0            0            0            0
    (>60dB)            0
avgNf:    -89, high:  -58, low:  -90
Noise Floor profile [-100dB...-40dB]
          0            0            0          145          126
         11            2            0            1            0
          3            0            1            0            1
          0            0            0            0            0
    (>-40dB)           0
avgRssi:   51, high:   53, low:   50
RSSI profile        [-100dB...-40dB]
          0            0            0            0            0
          0            0            0            0            0
          0            0            0            0            0
          0            7          283            0            0
    (>-40dB)           0
Summary PktFailedRate (Total pkts sent/recvd):                        0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%
```

次の表に、**config mesh linktest** コマンドで表示される出力フラグを示します。

表 *6 : Config Mesh Linktest* コマンドの出力フラグ

出力フラグ	説明
txPkts	ソースから送信されたパケット数。
txBuffAllocErr	発信元での linktest バッファ割り当てエラーの数（ゼロであると予想される）。
txQFullErrs	発信元での linktest キューフルエラーの数（ゼロであると予想される）。
Total rx pkts heard at destination	宛先で受信された linktest パケットの数（txPkts と同じまたは近似値であると予想される）。
rx pkts decoded correctly	宛先で受信され正しくデコードされた linktest パケットの数（txPkts と同じまたは近似値であると予想される）。
err pkts: Total	エラーのある linktest パケットのパケット エラー統計情報。
rx lost packets	宛先で受信されない linktest パケットの総数。
rx dup pkts	宛先で受信した重複 linktest パケットの総数。
rx out of order	宛先で順序が入れ替わって受信された linktest パケットの総数。
avgNF	平均ノイズ フロア。
Noise Floor profile	ノイズフロアのプロファイル（dB 単位）は負の数値です。
avgSNR	平均 SNR 値。
SNR profile [odb...60dB]	0～60 dB の間で受信したヒストグラムのサンプル。SNR プロファイルの異なる列はバケット 0-3、3-6、6-9、最大 57-60 を下回るパケット数です。
avgRSSI	平均 RSSI 値。平均の上限および下限 RSSI 値は正の数値です。
RSSI profile [-100dB...-40dB]	RSSI プロファイル（dB 単位）は負の数値です。

config mesh lsc

メッシュ アクセス ポイントのローカルで有効な証明書（LSC）を設定するには、**config mesh lsc** コマンドを使用します。

config mesh lsc {**enable** | **disable**}

構文の説明

enable	メッシュ アクセス ポイントの LSC を有効にします。
disable	メッシュ アクセス ポイントの LSC を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メッシュ アクセス ポイントの LSC を有効にする例を示します。

```
(Cisco Controller) >config mesh lsc enable
```

config mesh lsc advanced

メッシュ アクセス ポイント（AP）の外部認証、認可、およびアカウンティング（AAA）サーバでワイルド カードが使用されている場合に高度な LSC（ローカルで有効な証明書）を設定するには、**config mesh lsc advanced** コマンドを使用します。

config mesh lsc advanced {**enable** | **disable**}

構文の説明

enable	メッシュ AP の高度な LSC を有効にします。
disable	メッシュ AP の高度な LSC を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、メッシュ AP の高度な LSC を有効にする例を示します。

```
(Cisco Controller) >config  mesh lsc advanced enable
```

config mesh lsc advanced ap-provision

メッシュ アクセス ポイント（AP）の外部認証、認可、およびアカウンティング（AAA）サーバでワイルドカードが使用されている場合に高度なメッシュ LSC（ローカルで有効な証明書）AP プロビジョニングを設定するには、**config mesh lsc advanced ap-provision** コマンドを使用します。

config mesh lsc advanced ap-provision {**enable** | **disable** | **open-window** {**enable** | **disable**} | **provision-controller** {**enable** | **disable**}}

構文の説明

enable	メッシュ AP の外部 AAA サーバでワイルド カードが使用されている場合に高度なメッシュ LSC AP プロビジョニングを有効にします。
disable	メッシュ AP の外部 AAA サーバでワイルド カードが使用されている場合に高度なメッシュ LSC AP プロビジョニングを無効にします。
open-window	MAC 検証なしですべてのメッシュ AP のメッシュ LSC プロビジョニングを設定します。
enable	MAC 検証なしですべてのメッシュ AP の AP プロビジョニングを有効にします。
disable	MAC 検証なしですべてのメッシュ AP の AP プロビジョニングを無効にします。
provision-controller	LSC を取得するためにメッシュ AP のプロビジョニング コントローラ詳細情報を設定します。
enable	LSC を取得するためのプロビジョニング コントローラ オプションを有効にします。
disable	LSC を取得するためのプロビジョニング コントローラ オプションを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、高度な AP プロビジョニング方式を有効にする例を示します。

```
(Cisco Controller) >config mesh lsc advanced ap-provision enable
```

config mesh multicast

マルチキャスト モード設定を行って、メッシュ ネットワーク内のマルチキャスト送信を管理するには、**config mesh multicast** コマンドを使用します。

config mesh multicast {**regular** | **in** | **in-out**}

構文の説明

regular	ブリッジが有効に設定されているルート アクセス ポイント（RAP）およびメッシュ アクセス ポイント（MAP）によって、メッシュ ネットワーク全体とすべてのセグメントにビデオをマルチキャストします。
in	MAP によってイーサネット マップから RAP のイーサネット ネットワークに受信されたマルチキャスト ビデオを転送します。これ以上の転送は行われないので、RAP で受信された LWAPP 以外のマルチキャストがメッシュ ネットワーク内の MAP イーサネット ネットワーク（マルチキャストの発生元）に送り返されることはありません。また、MAP-to-MAP マルチキャストは除外されているので、このようなマルチキャストは発生しません。
in-out	RAP と MAP をそれぞれを異なる方法でマルチキャストに設定します。 マルチキャスト パケットがイーサネット経由で MAP で受信された場合、RAP に送信されますが、他の MAP イーサネットには送信されません。MAP-to-MAP パケットはマルチキャストから除外されます。 マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。詳細については、「使用上のガイドライン」の項を参照してください。

コマンド デフォルト

In-out モード

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラ GUI を使用してメッシュ ネットワークのマルチキャストをイネーブルにすることはできません。

メッシュ マルチキャスト モードは、ブリッジが有効に設定されているアクセス ポイントのメッシュ アクセス ポイント（MAP）およびルート アクセス ポイント（RAP）がメッシュ ネットワーク内のイーサネット LAN 間でマルチキャストを送信する方法を決定します。メッシュ マルチキャスト モードは、LWAPP マルチキャスト以外のトラフィックだけを管理します。LWAPP マルチキャスト トラフィックは、別のメカニズムで管理されます。

コントローラ CLI を使用して 3 種類のメッシュ マルチキャスト モードを設定し、すべてのメッシュ アクセス ポイントでビデオ カメラ ブロードキャストを管理できます。イネーブルになっている場合、これらのモードは、メッシュ ネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

in-out モードを使用する場合、ネットワークを適切に区分けして、RAP が送信したマルチキャストを同一イーサネット セグメントの別の RAP が受信し、ネットワークに送り返さないようにすることが重要です。

（注） 802.11b クライアントでの CAPWAP マルチキャストの受信が必要な場合、マルチキャストは、コントローラおよびメッシュ ネットワーク（**config network multicast global** コマンドを使用）でグローバルに有効にする必要があります。マルチキャストをメッシュ ネットワーク外の 802.11b クライアントに伝送する必要がない場合、グローバルなマルチキャスト パラメータを無効にする必要があります。

次に、ブリッジが有効に設定されている RAP および MAP によってメッシュ ネットワーク全体とすべてのセグメントにビデオをマルチキャストする例を示します。

```
(Cisco Controller) >config mesh multicast regular
```

config mesh parent preferred

メッシュ アクセス ポイントに対して優先される親を設定するには、**config mesh parent preferred** コマンドを使用します。

config mesh parent preferred *cisco_ap* {*mac_address* | **none**}

構文の説明

cisco_ap	子のアクセス ポイントの名前。
mac_address	優先される親の MAC アドレス。
none	設定された親をクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

子の AP は、次の基準に基づいて優先される親を選択します。

- 優先される親は最良の親です。
- 優先される親には少なくとも 20 dB のリンク SNR があります（他の親はどんなに優れていても無視されます）。
- 優先される親には 12 dB ～ 20 dB の範囲内のリンク SNR がありますが、他の親が非常に優れていることはありません（つまり、SNR が 20 % 以上優れている）。SNR が 12 dB 未満の場合、設定は無視されます。
- 優先される親はブラックリストに掲載されません。
- 優先される親は、12 dB ～ 20 dB の範囲内の（DFS）のため、サイレント モードになりません。
- 優先される親は同じブリッジ グループ名（BGN）に属します。設定された優先される親が同じ BGN に属さず、他の親が利用可能でない場合、子はデフォルトの BGN を使用して親 AP に join します。

次に、メッシュ アクセス ポイント myap1 に対して MAC アドレスが 00:21:1b:ea:36:60 である優先される親を設定する例を示します。

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60
```

次に、キーワード none を使用して、メッシュ アクセス ポイント myap1 に対して MAC アドレスが 00:21:1b:ea:36:60 である優先される親をクリアする例を示します。

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60 none
```

config mesh public-safety

メッシュ アクセス ポイント用に 4.9 GHz の Public Safety 帯域を有効または無効にするには、**config mesh public-safety** コマンドを使用します。

config mesh public-safety {**enable** | **disable**} {**all** | *cisco_ap* }

構文の説明

enable	4.9 GHz の Public Safety 帯域を有効にします。
disable	4.9 GHz の Public Safety 帯域を無効にします。
all	すべてのメッシュ アクセス ポイントにこのコマンドを適用します。
cisco_ap	特定のメッシュ アクセス ポイント。

コマンド デフォルト

4.9 GHz の Public Safety 帯域は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

4.9 GHz は、公共安全（Public Safety）に関わる職員に使用が制限された認可周波数帯域です。

次に、すべてのメッシュ アクセス ポイントに 4.9 GHz の Public Safety 帯域を有効にする例を示します。

```
(Cisco Controller) >config mesh public-safety enable all
4.9GHz is a licensed frequency band in -A domain for public-safety usage
 Are you sure you want to continue? (y/N) y
```

config mesh radius-server

メッシュ アクセス ポイントの外部認証を有効または無効にするには、**config mesh radius-server** コマンドを入力します。

config mesh radius-server *index* {**enable** | **disable**}

構文の説明

index	RADIUS 認証方式。オプションは次のとおりです。 • メッシュ RADIUS サーバ設定に拡張可能認証プロトコル（EAP）を指定するには、**eap** と入力します。 • メッシュ RADIUS サーバ設定に事前共有キー（PSK）を指定するには、**psk** と入力します。
enable	メッシュ アクセス ポイントの外部認証を有効にします。
disable	メッシュ アクセス ポイントの外部認証を無効にします。

コマンド デフォルト

EAP は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メッシュ アクセス ポイントの外部認証を有効にする例を示します。

```
(Cisco Controller) >config mesh radius-server eap enable
```

config mesh range

屋外のルート アクセス ポイント（RAP）とメッシュ アクセス ポイント（MAP）の最大範囲をグローバルに設定するには、**config mesh range** コマンドを使用します。

config mesh range ［*distance*］

構文の説明

distance	（任意）メッシュ アクセス ポイントの最大動作範囲（150～132,000 フィート）。

コマンド デフォルト

12,000 フィート。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを有効にすると、すべての屋外メッシュ アクセス ポイントがリブートします。このコマンドは、屋内アクセス ポイントには影響しません。

次に、屋外のメッシュ RAP と MAP の範囲を設定する例を示します。

```
(Cisco Controller) >config mesh range 300
Command not applicable for indoor mesh. All outdoor Mesh APs will be rebooted
Are you sure you want to start? (y/N) y
```

config mesh secondary-backhaul

メッシュ ネットワークでセカンダリ バックホールを設定するには、**config mesh secondary-backhaul** コマンドを使用します。

config mesh secondary-backhaul {**enable** [**force-same-secondary-channel**] | **disable** [**rll-retransmit** | **rll-transmit**]}

構文の説明

enable	セカンダリ バックホール設定を有効にします。
force-same-secondary- channel	（任意）セカンダリ バックホール メッシュ機能を有効にします。最初のホップ ノードをルートとするすべてのアクセス ポイントが同じセカンダリ チャネルを持ち、2 番目以降のホップでのメッシュ アクセス ポイント（MAP）に対する自動または手動チャネル割り当てを無視するように強制します。
disable	セカンダリ バックホール設定を無効にします。
rll-transmit	（任意）2 番目以降のホップで Reliable Link Layer（RLL）を使用します。
rll-retransmit	（任意）信頼性向上のために RLL の再試行回数を増やします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、断続的な干渉のためにプライマリ バックホールで送信できないトラフィックの一時的なパスとしてセカンダリ バックホール無線を使用します。

次に、セカンダリ バックホール無線を有効にし、最初のホップ ノードをルートとするすべてのアクセス ポイントが同じセカンダリ チャネルを持つように強制する例を示します。

```
(Cisco Controller) >config mesh secondary-backhaul enable force-same-secondary-channel
```

config mesh security

メッシュ ネットワークのセキュリティ設定を行うには、**config mesh security** コマンドを使用します。

config mesh security {{**rad-mac-filter** | **force-ext-auth** | **lsc-only-auth**} {**enable** | **disable**}} | {{**eap** | **psk provisioning** | **provisioning window**} | {**enable** | **disable**}} | {**delete_psk** | **key**}

構文の説明

rad-mac-filter	メッシュ セキュリティ設定のリモート認証ダイヤルインユーザ サービス（RADIUS）MAC アドレス フィルタを有効にします。
force-ext-auth	メッシュ セキュリティ設定の強制外部認証を無効にします。
lsc-only-auth	メッシュ セキュリティ設定の LSC（ローカルで有効な証明書）のみの認証を有効にします。
enable	メッシュ セキュリティ設定を有効にします。
disable	メッシュ セキュリティ設定を無効にします。
eap	メッシュ セキュリティ設定に拡張可能認証プロトコル（EAP）をデフォルトで指定します。
psk	メッシュ セキュリティ設定に事前共有キー（PSK）を指定します。
provisioning	シスコ ワイヤレス コントローラ（WLC）で PSK のプロビジョニングを暗号化します。
provisioning window	Cisco WLC で PSK のプロビジョニング ウィンドウを暗号化します。
enable	PSK のプロビジョニングを有効にします。
disable	PSK のプロビジョニングを無効にします。
key	PSK のキーを指定します。

コマンド デフォルト

メッシュ セキュリティについては EAP がデフォルトとして指定されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.2	このコマンドが変更され、PSK プロビジョニングと PSK プロビジョニング キーワードが追加されました。

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして EAP を設定する例を示します。

```
(Cisco Controller) config mesh security eap
```

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして PSK を設定する例を示します。

```
(Cisco Controller) config mesh security psk
```

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして PSK プロビジョニングを有効にする例を示します。

```
(Cisco Controller)> config mesh security psk provisioning enable
```

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして PSK プロビジョニング キーを設定する例を示します。

```
(Cisco Controller)> config mesh security psk provisioning key 5
```

次に、すべてのメッシュ アクセス ポイントのセキュリティ オプションとして PSK プロビジョニング ウィンドウを有効にする例を示します。

```
(Cisco Controller)> config mesh security psk provisioning window enable
```

次に、Cisco WLC の PSK プロビジョニングを削除する例を示します。

```
(Cisco Controller)> config mesh security psk provisioning delete_psk wlc
```

次に、すべてのメッシュ アクセス ポイントの PSK プロビジョニングを削除する例を示します。

```
(Cisco Controller)> config mesh security psk provisioning delete_psk ap
```

次に、Cisco WLC のすべての設定から PSK プロビジョニングを削除する例を示します。

```
(Cisco Controller)> config mesh security psk provisioning delete_psk wlc all
```

config mesh slot-bias

シリアル バックホール メッシュ アクセス ポイントのスロット バイアスを有効または無効にするには、**config mesh slot-bias** コマンドを使用します。

config mesh slot-bias {**enable** | **disable**}

構文の説明

enable	シリアル バックホール メッシュ AP のスロット バイアスを有効にします。
disable	シリアル バックホール メッシュ AP のスロット バイアスを無効にします。

コマンド デフォルト

デフォルトでは、スロット バイアスが有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用する場合、次のガイドラインに従ってください。

- **config mesh slot-bias** コマンドはグローバル コマンドであるため、同じコントローラにアソシエートされたすべての 1524SB AP に適用できます。
- スロット バイアスは、スロット 1 とスロット 2 の両方が使用可能である場合にのみ適用できます。動的周波数選択（DFS）のため、スロット無線に利用可能なチャネルがない場合は、他のスロットがアップリンクとダウンリンク両方の役割を担います。
- ハードウェアの問題のため、スロット 2 が利用可能でない場合でも、スロット バイアスは通常どおり機能します。スロット バイアスを無効にするか、アンテナを修復して是正処置を実行する必要があります。

次に、シリアル バックホール メッシュ AP のスロット バイアスを無効にする例を示します。

```
(Cisco Controller) >config mesh slot-bias disable
```

config mgmtuser add

コントローラにローカル管理ユーザを追加するには、**config mgmtuser add** コマンドを使用します。

config mgmtuser add *username password* {**lobby-admin** | **read-write** | **read-only**} [*description*]

構文の説明

username	アカウントユーザ名。ユーザ名には、最大24文字の英数字を使用できます。
password	アカウントパスワード。パスワードには、最大24文字の英数字を使用できます。
read-write	読み取りと書き込みアクセス権を持つ管理ユーザを作成します。
read-only	読み取り専用アクセス権を持つ管理ユーザを作成します。
description	（任意）アカウントについての説明。説明には、最大32文字の英数字を使用できます。説明は二重引用符で囲みます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、読み取りと書き込みアクセス権を持つ管理ユーザ アカウントを作成する例を示します。

```
(Cisco Controller) > config mgmtuser add admin admin read-write "Main account"
```

関連コマンド

show mgmtuser

config mgmtuser delete

コントローラからローカル管理ユーザを削除するには、**config mgmtuser delete** コマンドを使用します。

config mgmtuser delete *username*

構文の説明

username	アカウントユーザ名。ユーザ名には、最大24文字の英数字を使用できます。

コマンド デフォルト

管理ユーザは、デフォルトでは削除されません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、コントローラから管理ユーザ アカウントの管理者を削除する例を示します。

```
(Cisco Controller) > config mgmtuser delete admin

Deleted user admin
```

関連コマンド

show mgmtuser

config mgmtuser description

コントローラの既存の管理ユーザ ログインに説明を追加するには、**config mgmtuser description** コマンドを使用します。

config mgmtuser description *username description*

構文の説明

username	アカウント ユーザ名。ユーザ名には、最大 24 文字の英数字を使用できます。
description	アカウントの説明。説明には、最大 32 文字の英数字を使用できます。説明は二重引用符で囲みます。

コマンド デフォルト

管理ユーザに説明が追加されません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、管理ユーザ「admin」に説明「master-user」を追加する例を示します。

```
(Cisco Controller) > config mgmtuser description admin "master user"
```

関連コマンド

config mgmtuser add

config mgmtuser delete

config mgmtuser password

show mgmtuser

config mgmtuser password

管理ユーザ パスワードを設定するには、**config mgmtuser password** コマンドを使用します。

config mgmtuser password *username password*

構文の説明

username	アカウントユーザ名。ユーザ名には、最大24文字の英数字を使用できます。
password	アカウント パスワード。パスワードには、最大 24 文字の英数字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、新しいパスワード5rTfmを使用して、管理ユーザ「admin」のパスワードを変更する例を示します。

```
(Cisco Controller) > config mgmtuser password admin 5rTfm
```

関連コマンド

show mgmtuser

config mgmtuser telnet

ローカル管理ユーザによる Cisco ワイヤレス LAN コントローラへの接続での Telnet を使用を有効にするには、**config mgmtuser telnet** コマンドを使用します。

config mgmtuser telnet *user_name* {**enable** | **disable**}

構文の説明

user_name	ローカル管理ユーザのユーザ名。
enable	ローカル管理ユーザによる Cisco WLC への接続での Telnet の使用を有効にします。最大 24 文字の英数字を入力できます。
disable	ローカル管理ユーザによる Cisco WLC への接続での Telnet の使用を無効にします。

コマンド デフォルト

ローカル管理ユーザは Telnet を使用して Cisco WLC に接続できます。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

このコマンドを有効にするにはグローバルTelnetを有効にする必要があります。このオプションを有効にしてもセキュア シェル（SSH）接続は影響を受けません。

次に、ローカル管理ユーザによる Cisco WLC への接続での Telnet の使用を有効にする例を示します。

```
(Cisco Controller) > config mgmtuser telnet admin1 enable
```

config mgmtuser termination-interval

ユーザの再認証終了間隔 (秒単位) を設定するには、**config mgmtuser termination-interval** コマンドを使用します。

config mgmtuser termination-interval {*seconds* }

構文の説明

seconds	ユーザがログアウトするまでの再認証終了間隔（秒単位）。デフォルト値は 0、有効な範囲は 0 ～ 300 秒です。

コマンド履歴

リリース	変更内容
8.2	このコマンドは本リリースで追加されました。

次に、ユーザがログアウトするまでの間隔（秒単位）を設定する例を示します。

```
(Cisco Controller) > config mgmtuser termination-interval 180
```

config mobility dscp

モビリティ コントローラ間の DSCP 値を設定するには、**config mobility dscp** コマンドを使用します。

config mobility dscp *dscp_value*

構文の説明

dscp_value	0～63 の DSCP 値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ コントローラ間の DSCP 値を 40 に設定する例を示します。

```
(Cisco Controller) >config mobility dscp 40
```

config mobility group anchor

WLAN または有線ゲスト LAN の新しいモビリティ アンカーを作成するには、**config mobility group anchor** コマンドを使用します。

config mobility group anchor {**add** | **delete**} {**wlan** *wlan_id* | **guest-lan** *guest_lan_id*} *anchor_ip*

構文の説明

add	無線 LAN にモビリティ アンカーを追加または変更します。
delete	無線 LAN からモビリティ アンカーを削除します。
wlan	無線 LAN のアンカー設定を指定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
guest-lan	ゲスト LAN のアンカー設定を指定します。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子。
anchor_ip	アンカー コントローラの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

wlan_id または *guest_lan_id* は必ず指定し、無効にする必要があります。

1 つ目のモビリティ アンカーを設定するときに、WLAN または有線ゲスト LAN で自動アンカー モビリティを有効にします。最後のアンカーを削除すると、自動アンカー モビリティ機能は無効になり、新しいアソシエーションに対しては標準のモビリティが再度使用されるようになります。

次に、無線 LAN ID 2 に IP アドレス 192.12.1.5 のモビリティ アンカーを追加する例を示します。

```
(Cisco Controller) >config mobility group anchor add wlan 2 192.12.1.5
```

次に、無線 LAN から IP アドレス 193.13.1.15 のモビリティ アンカーを削除する例を示します。

```
(Cisco Controller) >config mobility group anchor delete wlan 5 193.13.1.5
```

config mobility group domain

モビリティ ドメイン名を設定するには、**config mobility group domain** コマンドを使用します。

config mobility group domain *domain_name*

構文の説明

domain_name	ドメイン名。ドメイン名は最大31文字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、モビリティ ドメイン名 lab1 を設定する例を示します。

```
(Cisco Controller) >config mobility group domain lab1
```

config mobility group keepalive count

エラーが発生したモビリティ グループ メンバー（アンカー Cisco WLC を含む）を検出するように Cisco WLC を設定するには、**config mobility group keepalive count** コマンドを使用します。

config mobility group keepalive count *count*

構文の説明

count	モビリティ グループ メンバーに ping 要求を送信する回数。この回数を超えると、メンバーにはアクセスできないと見なされます。有効な範囲は 3 ～ 20 です。デフォルトは 3 です。

コマンド デフォルト

モビリティ グループ メンバーに ping 要求を送信するデフォルトの回数は 3 回です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ グループ メンバーに ping 要求を送信する回数を 3 回に指定する方法の例を示します。この回数を超えると、メンバーにはアクセスできないと見なされます。

```
(Cisco Controller) >config mobility group keepalive count 3
```

config mobility group keepalive interval

エラーが発生したモビリティ グループ メンバー（アンカー コントローラを含む）を検出するようにコントローラを設定するには、**config mobility group keepalive** コマンドを使用します。

config mobility group keepalive *interval*

構文の説明

interval	モビリティ グループ メンバーへの ping 要求の送信間隔。範囲は 1 ～ 30 秒です。デフォルト値は 10 秒です。

コマンド デフォルト

ping 要求のデフォルトの送信間隔は 10 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ グループ メンバーに ping 要求を送信する間隔を 10 秒に指定する例を示します。

```
(Cisco Controller) >config mobility group keepalive 10
```

config mobility group member

モビリティ グループのメンバー リストのユーザを追加または削除するには、**config mobility group member** コマンドを使用します。

config mobility group member {**add** *MAC-addr IP-addr* [*group_name*] | **delete** *MAC-addr* | **hash** *IP-addr* {*key* | **none**}}

構文の説明

add	リストのモビリティ グループ メンバーを追加または変更します。
mac-addr	メンバー スイッチの MAC アドレス。
IP-addr	メンバー スイッチの IP アドレス。
group_name	（任意）メンバー スイッチ グループ名（デフォルトのグループ名と異なる場合）。
delete	（任意）リストからモビリティ グループ メンバーを削除します。
hash	認証のためにハッシュ キーを設定します。メンバーが同じ仮想ドメインのコントローラである場合だけ、ハッシュキーを設定できます。
key	仮想コントローラのハッシュ キー。たとえば、a819d479dcfeb3e0974421b6e8335582263d9169 のようになります。
none	仮想コントローラの以前のハッシュ キーをクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、IPv4 アドレスを持つモビリティ グループ メンバーをリストに追加する例を示します。

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 209.165.200.225
```

次に、IPv6アドレスを持つモビリティ グループ メンバーをリストに追加する例を示します。

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 2001:DB8::1
```

次に、同じドメインの仮想コントローラのハッシュ キーを設定する例を示します。

（注） この例の IP アドレスには、IPv4 または IPv6 のいずれかの形式を使用できます。

```
(Cisco Controller) >config mobility group member hash 209.165.201.1
a819d479dcfeb3e0974421b6e8335582263d9169
```

config mobility group multicast-address

モビリティ リスト内の非ローカル グループに対して、マルチキャスト グループ IP アドレスを設定するには、**config mobility group multicast-address** コマンドを使用します。

config mobility group multicast-address *group_name ip_address*

構文の説明

group_name	メンバ スイッチ グループ名（デフォルトのグループ名と異なる場合）。
ip_address	メンバ スイッチの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、test という名前のグループに対して、マルチキャスト グループの IP アドレス 10.10.10.1 を設定する例を示します。

```
(Cisco Controller) >config mobility group multicast-address test 10.10.10.1
```

次に、test という名前のグループに対して、マルチキャスト グループの IP アドレス 2001:DB8::1 を設定する例を示します。

```
(Cisco Controller) >config mobility group multicast-address test 2001:DB8::1
```

config mobility multicast-mode

モビリティ マルチキャスト モードを有効または無効にするには、**config mobility multicast-mode** コマンドを使用します。

config mobility multicast-mode {**enable** | **disable**} *local_group_multicast_address*

構文の説明

enable	マルチキャストモードをイネーブルにします。この場合、コントローラはマルチキャストモードを使用して、Mobile Announce メッセージをローカル グループへ送信します。
disable	マルチキャスト モードをディセーブルにします。この場合、コントローラはユニキャストモードを使用して、Mobile Announce メッセージをローカル グループへ送信します。
local_group_multicast_address	ローカル モビリティ グループの IP アドレス。

コマンド デフォルト

モビリティ マルチキャスト モードは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ローカル モビリティ グループの IP アドレス 157.168.20.0 に対して、マルチキャスト モビリティ モードを有効にする例を示します。

```
(Cisco Controller) >config mobility multicast-mode enable 157.168.20.0
```

config mobility new-architecture

Cisco ワイヤレス LAN コントローラ（WLC） で新しいモビリティを有効にするには、**config mobility new-architecture** コマンドを使用します。

config mobility new-architecture {**enable** | **disable**}

構文の説明

enable	新しいモビリティ アーキテクチャに切り替えるように Cisco WLC を設定します。
disable	古いフラット モビリティ アーキテクチャに切り替えるように Cisco WLC を設定します。

コマンド デフォルト

デフォルトでは、新しいモビリティは無効になっています。

コマンド履歴

リリース	変更内容
7.3.112.0	このコマンドが導入されました。

使用上のガイドライン

新しいモビリティは、Cisco WiSM2、Cisco 2500 シリーズ ワイヤレス コントローラ、Cisco 5500 シリーズ ワイヤレス コントローラ、および Cisco 8500 シリーズ ワイヤレス コントローラでのみサポートされています。新しいモビリティは、Cisco Catalyst 3850 シリーズや Cisco 5760 ワイヤレス LAN コントローラなどのワイヤレス コントロール モジュール（WCM）を使用した統合アクセス コントローラとの互換性を Cisco WLC で実現します。

次に、Cisco WLC で新しいモビリティを有効にする例を示します。

```
(Cisco Controller) >config mobility new-architecture enable
```

config mobility oracle

Mobility Oracle（MO）を設定するには、**config mobility oracle** コマンドを使用します。

config mobility oracle {**enable** | **disable** | **ip** *ip_address* }

構文の説明

enable	起動時に MO を有効にします。
disable	起動時に MO を無効にします。
ip	MO の IP アドレスを指定します。
ip_address	MO の IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.3.112.0	このコマンドが導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

使用上のガイドライン

MO は 1 つの完全なモビリティ ドメインの下で、クライアント データベースを保持します。これは、ステーション データベース、モビリティ Cisco WLC へのインターフェイス、および NTP サーバで構成されます。モビリティ ドメイン全体に MO は 1 つのみです。

このコマンドでは IPv6 アドレス形式はサポートされません。

次に、MO の IP アドレスを設定する例を示します。

```
(Cisco Controller) >config mobility oracle ip 27.0.0.1
```

config mobility secure-mode

Cisco WLC 間でやり取りするモビリティ メッセージにセキュア モードを設定するには、**config mobility secure-mode** コマンドを使用します。

config mobility secure-mode {**enable** | **disable**}

構文の説明

enable	モビリティ グループのメッセージ セキュリティをイネーブルにします。
disable	モビリティ グループのメッセージ セキュリティをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ メッセージのセキュア モードを有効にする例を示します。

```
(Cisco Controller) >config mobility secure-mode enable
```

config mobility statistics reset

モビリティの統計情報をリセットするには、**config mobility statistics reset** コマンドを使用します。

config mobility statistics reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ グループの統計情報をリセットする例を示します。

```
(Cisco Controller) >config mobility statistics reset
```

config netuser add

コントローラ上のローカルユーザデータベースにWLAN上のゲストユーザまたは有線ゲストLANを追加するには、**config netuser add** コマンドを使用します。

config netuser add *username password* {**wlan** *wlan_id* | **guestlan** *guestlan_id*} **userType guest lifetime** *lifetime* **description** *description*

構文の説明

username	ゲストユーザ名。ユーザ名には、最大50文字の英数字を使用できます。
password	ユーザパスワード。パスワードには、最大24文字の英数字を使用できます。
wlan	関連付ける無線LANの識別子を指定するか、すべての無線 LAN にゼロを指定します。
wlan_id	ユーザに割り当てられている無線 LAN 識別子。値 0 の場合、ユーザをすべての無線 LAN にアソシエートします。
guestlan	関連付けるゲスト LAN の識別子を指定するか、すべての無線LANにゼロを指定します。
guestlan_id	ゲスト LAN の ID。
userType	ユーザ タイプを指定します。
guest	ゲスト ユーザのゲストを指定します。
lifetime	ライフタイムを指定します。
lifetime	ゲスト ユーザの秒単位のライフタイム値（60 ～ 259200 または 0）。 （注） 値 0 は、ライフタイム値が無制限であることを示します。
description	ユーザの簡単な説明。説明は二重引用符で囲み、最大 32 文字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

ローカル ネットワーク ユーザは 1 つのデータベースに格納されるので、これらのユーザ名は重複してはいけません。

次に、永久ユーザ名 Jane をワイヤレス ネットワークに 1 時間追加する例を示します。

```
(Cisco Controller) > config netuser add jane able2 1 wlan_id 1 userType permanent
```

次に、ゲスト ユーザ名 George をワイヤレス ネットワークに 1 時間追加する例を示します。

```
(Cisco Controller) > config netuser add george able1 guestlan 1 3600
```

関連コマンド

show netuser

config netuser delete

config netuser delete

ローカル ネットワークから既存のユーザを削除するには、**config netuser delete** コマンドを使用します。

config netuser delete { **username** *username* | **wlan-id** *wlan-id*}

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、最大 24 文字の英数字を使用できます。
wlan-id	WLAN ID 番号。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ローカル ネットワーク ユーザは 1 つのデータベースに格納されるので、これらのユーザ名は重複してはいけません。

（注） ネットワーク ユーザに関連付けられている WLAN を削除すると、システムは、先に WLAN に関連付けられているすべてのネットワーク ユーザを削除するように指示するプロンプトを表示します。ネットワーク ユーザを削除した後に、WLAN を削除できます。

次に、既存のユーザ名 able1 をネットワークから削除する例を示します。

```
(Cisco Controller) > config netuser delete able1
Deleted user able1
```

関連コマンド

show netuser

config netuser description

既存のネットワーク ユーザに説明を追加するには、**config netuser description** コマンドを使用します。

config netuser description *username description*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、最大 24 文字の英数字を使用できます。
description	（任意）ユーザの説明。説明は二重引用符で囲み、最大 32 文字の英数字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ユーザの説明「HQ1 Contact」を既存のネットワーク ユーザ名 able 1 に追加する例を示します。

```
(Cisco Controller) > config netuser description able1 "HQ1 Contact"
```

関連コマンド

show netuser

config netuser guest-lan-id

ネットワーク ユーザの有線ゲスト LAN ID を設定するには、**config netuser guest-lan-id** コマンドを使用します。

config netuser guest-lan-id *username lan_id*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、24 文字の英数字を指定できます。
lan_id	ユーザと関連付けるための有線ゲスト LAN の ID。値が 0 の場合、ユーザはすべての有線 LAN に関連付けられます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、有線 LAN ID 2 を aire1 という名前のユーザに関連付けるように設定する例を示します。

```
(Cisco Controller) > config netuser guest- lan-id aire1 2
```

関連コマンド

show netuser

show wlan summary

config netuser guest-role apply

ゲスト ユーザに Quality of Service（QoS）のロールを適用するには、**config netuser guest-role apply** コマンドを使用します。

config netuser guest-role apply *username role_name*

構文の説明

username	ユーザ名。
role_name	QoS ゲスト ロール名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ゲスト ユーザに QoS ロールを割り当てない場合、[User Details] の [Role] フィールドにデフォルトとしてロールが示されます。このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

ゲスト ユーザの QoS ロールの割り当てを解除する場合は、**config netuser guest-role apply** *username* **default** を使用します。今後、このユーザについては WLAN の QoS プロファイルで定義された帯域幅コントラクトが使用されます。

次に、Contractor という名前の QoS ゲスト ロールを持つゲスト ユーザ jsmith QoS ロールを適用する例を示します。

```
(Cisco Controller) > config netuser guest-role apply jsmith Contractor
```

関連コマンド

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role create

ゲスト ユーザの Quality of Service（QoS）ロールを作成するには、**config netuser guest-role create** コマンドを使用します。

config netuser guest-role create *role_name*

構文の説明

role name	QoS ゲスト ロール名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

QoS ロールを削除するには、**config netuser guest-role delete** *role-name* を使用します。

次に、guestuser1 という名前のゲスト ユーザに QoS ロールを作成する例を示します。

```
(Cisco Controller) > config netuser guest-role create guestuser1
```

関連コマンド

config netuser guest-role delete

config netuser guest-role delete

ゲスト ユーザの Quality of Service（QoS）のロールを削除するには、**config netuser guest-role delete** コマンドを使用します。

config netuser guest-role delete *role_name*

構文の説明

role name	Quality of Service（QoS）ゲスト ロール名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、guestuser1 の Quality of Service（QoS）のロールを削除する例を示します。

```
(Cisco Controller) > config netuser guest-role delete guestuser1
```

関連コマンド

config netuser guest-role create

config netuser guest-role qos data-rate average-data-rate

ユーザ 1 人あたりの TCP トラフィックの平均データ レートを設定するには、**config netuser guest-role qos data-rate average-data-rate** コマンドを使用します。

config netuser guest-role qos data-rate average-data-rate *role_name rate*

構文の説明

role_name	Quality of Service（QoS）ゲスト ロール名。
rate	ユーザ 1 人あたりの TCP トラフィック レート。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意に識別するものです（contractor、vendor など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

次に、guestuser1 という名前の QoS ゲストの平均レートを設定する例を示します。

```
(Cisco Controller) > config netuser guest-role qos data-rate average-data-rate guestuser1
 0
```

関連コマンド

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role qos data-rate burst-data-rate

config netuser guest-role qos data-rate average-realtime-rate

ユーザ 1 人あたりの TCP トラフィックの平均データ レートを設定するには、**config netuser guest-role qos data-rate average-realtime-rate** コマンドを使用します。

config netuser guest-role qos data-rate average-realtime-rate *role_name rate*

構文の説明

role_name	Quality of Service（QoS）ゲスト ロール名。
rate	ユーザ 1 人あたりの TCP トラフィック レート。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意に識別するものです（contractor、vendor など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

次に、TCP トラフィックのレートが 0 Kbps である guestuser1 という名前の QoS ゲスト ユーザに対して平均データ レートを設定する例を示します。

```
(Cisco Controller) > config netuser guest-role qos data-rate average-realtime-rate
guestuser1 0
```

関連コマンド

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

ユーザ 1 人あたりの TCP トラフィックの最大データ レートを設定するには、**config netuser guest-role qos data-rate burst-data-rate** コマンドを使用します。

config netuser guest-role qos data-rate burst-data-rate *role_name rate*

構文の説明

role_name	Quality of Service（QoS）ゲスト ロール名。
rate	ユーザ 1 人あたりの TCP トラフィック レート。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

バーストデータ レートは平均データ レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意に識別するものです（contractor、vendor など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

次に、TCP トラフィックのレートが 0 Kbps である guestuser1 という名前の QoS ゲスト に対してピーク データ レートを設定する例を示します。

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-data-rate guestuser1
 0
```

関連コマンド

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-realtime-rate

ユーザ 1 人あたりの UDP トラフィックのバースト リアルタイム データ レートを設定するには、**config netuser guest-role qos data-rate burst-realtime-rate** コマンドを使用します。

config netuser guest-role qos data-rate burst-realtime-rate *role_name rate*

構文の説明

role_name	Quality of Service（QoS）ゲスト ロール名。
rate	ユーザ 1 人あたりの TCP トラフィック レート。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

バースト リアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、Quality of Service（QoS）ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意に識別するものです（contractor、vendor など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

次に、TCP トラフィックのレートが 0 Kbps である guestuser1 という名前の QoS ゲスト ユーザに対してバースト リアルタイム レートを設定する例を示します。

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-realtime-rate guestuser1
 0
```

関連コマンド

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

config netuser lifetime

ゲスト ネットワーク ユーザのライフタイムを設定するには、**config netuser lifetime** コマンドを使用します。

config netuser lifetime *username time*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、最大 50 文字の英数字を使用できます。
time	60 ～ 31536000 秒のライフタイム、または制限なしの場合は 0。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ゲストのネットワーク ユーザのライフタイムを設定する例を示します。

```
(Cisco Controller) > config netuser lifetime guestuser1 22450
```

関連コマンド

show netuser

show wlan summary

config netuser maxUserLogin

ネットワーク ユーザが利用できるログイン セッションの最大数を設定するには、**config netuser maxUserLogin** コマンドを使用します。

config netuser maxUserLogin *count*

構文の説明

count	単一ユーザの最大ログイン セッション数。指定できる値は 0（無制限）～ 8 です。

コマンド デフォルト

デフォルトでは、単一ユーザの最大ログイン セッション数は 0（無制限）です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、単一のユーザのログイン セッションの最大回数を 8 に設定する例を示します。

```
(Cisco Controller) > config netuser maxUserLogin 8
```

関連コマンド

show netuser

config netuser password

ローカル ネットワーク ユーザのパスワードを変更するには、**config netuser password** コマンドを使用します。

config netuser password *username password*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、最大 24 文字の英数字を使用できます。
password	ネットワーク ユーザ パスワード。パスワードには、最大 24 文字の英数字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、aire1 から aire2 にネットワーク ユーザ パスワードを変更する例を示します。

```
(Cisco Controller) > config netuser password aire1 aire2
```

関連コマンド

show netuser

config netuser wlan-id

ネットワーク ユーザの無線 LAN ID を設定するには、**config netuser wlan-id** コマンドを使用します。

config netuser wlan-id *username wlan_id*

構文の説明

username	ネットワーク ユーザ名。ユーザ名には、24 文字の英数字を指定できます。
wlan_id	ユーザとアソシエートする無線LAN識別子。値 0 の場合、ユーザをすべての無線 LAN にアソシエートします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

例

次に、無線 LAN ID 2 を aire1 という名前のユーザに関連付けるように設定する例を示します。

```
(Cisco Controller) > config netuser wlan-id aire1 2
```

関連コマンド

show netuser

show wlan summary

config network client-ip-conflict-detection

ネットワークのクライアント DHCP アドレス競合検出を有効または無効にするには、**config network client-ip-conflict-detection** コマンドを使用します。

config network client-ip-conflict-detection {**enable** | **disable**}

構文の説明

enable	ワイヤレス クライアントが、すでに別のクライアントに登録されている DHCP アドレスを受信した場合、以前のクライアントは切断されるため、そのクライアントは再接続して新しいアドレスを取得する必要があります。
disable	この機能をディセーブルにします。

コマンド デフォルト

ディセーブル

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

config network bridging-shared-secret

ブリッジの共有キーを設定するには、**config network bridging-shared-secret** コマンドを使用します。

config network bridging-shared-secret *shared_secret*

構文の説明

shared_secret	ブリッジの共有キーの文字列。文字列には 10 バイトまで使用できます。

コマンド デフォルト

ブリッジの共有キーは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、スイッチに接続するメッシュ アクセス ポイントのバックホール ユーザ データを暗号化する共有キーが作成されます。

このコマンドを機能させるには、zero touch configuration をイネーブルにしておく必要があります。

次に、ブリッジの共有キーの文字列「shhh1」を設定する例を示します。

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

関連コマンド

show network summary

config network web-auth captive-bypass

ネットワーク レベルでキャプティブ ポータルのバイパスをサポートするようにコントローラを設定するには、**config network web-auth captive-bypass** コマンドを使用します。

config network web-auth captive-bypass {**enable** | **disable**}

構文の説明

enable	コントローラがキャプティブ ポータルのバイパスをサポートできるようにします。
disable	コントローラがキャプティブ ポータルのバイパスをサポートできないようにします。

コマンド デフォルト

なし

次に、キャプティブ ポータルのバイパスをサポートするようにコントローラを設定する例を示します。

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

関連コマンド

show network summary

config network web-auth cmcc-support

config network web-auth port

ネットワーク レベルの Web 認証に関して追加ポートがリダイレクトされるように設定するには、**config network web-auth port** コマンドを使用します。

config network web-auth port *port*

構文の説明

port	ポート番号。有効な範囲は 0 ～ 65535 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web 認証に関して、追加ポート番号 1200 がリダイレクトされるように設定する例を示します。

```
(Cisco Controller) > config network web-auth port 1200
```

関連コマンド

show network summary

config network web-auth proxy-redirect

Web認証クライアントのプロキシのリダイレクションサポートを設定するには、**config network web-auth proxy-redirect** コマンドを使用します。

config network web-auth proxy-redirect {**enable** | **disable**}

構文の説明

enable	Web 認証クライアントのプロキシ リダイレクションをサポートできるようにします。
disable	Web 認証クライアントのプロキシ リダイレクションをサポートできないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

関連コマンド

show network summary

config network web-auth secureweb

クライアントにセキュア Web（https）認証を設定するには、**config network web-auth secureweb** コマンドを使用します。

config network web-auth secureweb {**enable** | **disable**}

構文の説明

enable	クライアントにセキュア Web（https）認証を行えるようにします。
disable	クライアントにセキュア Web（https）認証を行えないようにします。クライアントの HTTP Web 認証を有効にします。

コマンド デフォルト

デフォルトでは、クライアントのセキュア Web（https）認証は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config network web-auth secureweb disable コマンドを使用してクライアントのセキュア Web（https）認証を設定する場合、Cisco WLC をリブートして変更を適用する必要があります。

次に、クライアントに対してセキュア Web（https）認証を有効にする例を示します。

```
(Cisco Controller) > config network web-auth secureweb enable
```

関連コマンド

show network summary

config network webmode

Web モードを有効または無効にするには、**config network webmode** コマンドを使用します。

config network webmode {**enable** | **disable**}

構文の説明

enable	Webインターフェイスをイネーブルにします。
disable	Web インターフェイスをディセーブルにします。

コマンド デフォルト

Web モードのデフォルト値は **enable** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web インターフェイス モードを無効にする例を示します。

```
(Cisco Controller) > config network webmode disable
```

関連コマンド

show network summary

config network web-auth

ネットワーク レベルの Web 認証オプションを設定するには、**config network web-auth** コマンドを使用します。

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

構文の説明

port	Web 認証リダイレクション用に追加ポートを設定します。
port-number	ポート番号（0 ～ 65535）。
proxy-redirect	Web 認証クライアントのプロキシ リダイレクション サポートを設定します。
enable	Web 認証クライアントのプロキシ リダイレクション サポートをイネーブルにします。 （注） Web 認証プロキシのリダイレクションは、ポート 80、8080、および 3128 に加え、ユーザ定義のポート 345 に対してイネーブルになります。
disable	Web 認証クライアントのプロキシ リダイレクション サポートをディセーブルにします。

コマンド デフォルト

ネットワーク レベルの Web 認証のデフォルト値は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

設定を有効にするには、システムをリセットする必要があります。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

関連コマンド

show network summary

show run-config

config qos protocol-type

config network 802.3-bridging

コントローラで 802.3 ブリッジを有効または無効にするには、**config network 802.3-bridging** コマンドを使用します。

config network 802.3-bridging {**enable** | **disable**}

構文の説明

enable	802.3 ブリッジをイネーブルにします。
disable	802.3 ブリッジをディセーブルにします。

コマンド デフォルト

デフォルトでは、コントローラで 802.3 ブリッジが無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラ ソフトウェア リリース 5.2 では、2100 シリーズベース コントローラ用のソフトウェアベースのフォワーディング アーキテクチャが新しいフォワーディング プレーン アーキテクチャになります。その結果、2100 シリーズコントローラおよびCiscoサービス統合型ルータ用 Cisco Wireless LAN Controller Network Module は、デフォルトで 802.3 パケットをブリッジします。したがって、802.3 ブリッジをディセーブルにできるのは、4400 シリーズ コントローラ、Cisco WiSM、および Catalyst 3750G Wireless LAN コントローラ スイッチだけです。

802.3 ブリッジのステータスを決定するには、**show netuser guest-roles** コマンドを入力します。

次に、802.3 ブリッジを有効にする例を示します。

```
(Cisco Controller) > config network 802.3-bridging enable
```

関連コマンド

show netuser guest-roles

show network

config network allow-old-bridge-aps

スイッチとアソシエートする古いブリッジ アクセス ポイントの機能を設定するには、**config network allow-old-bridge-aps** コマンドを使用します。

config network allow-old-bridge-aps {**enable** | **disable**}

構文の説明

enable	スイッチ アソシエーションをイネーブルにします。
disable	スイッチ アソシエーションをディセーブルにします。

コマンド デフォルト

スイッチ アソシエーションは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、古いブリッジアクセス ポイントをスイッチに関連付けるように設定する例を示します。

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

AP ディスカバリ応答で NAT IP を有効または無効にするには、**config network ap-discovery** コマンドを使用します。

config network ap-discovery nat-ip-only {**enable** | **disable**}

構文の説明

enable	NAT IP の使用をディスカバリ応答でのみイネーブルにします。
disable	ディスカバリ応答での NAT IP および非 NAT IP の両方の使用をイネーブルにします。

コマンド デフォルト

NAT IP の使用がディスカバリ応答でのみ有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config interface nat-address management コマンドが設定されている場合、このコマンドによって、CAPWAP ディスカバリ応答で送信されるアドレスが制御されます。

すべての AP がコントローラの NAT ゲートウェイの外側にある場合、**config network ap-discovery nat-ip-only enable** コマンドを入力して、管理 NAT アドレスのみを送信します。

コントローラが、NAT ゲートウェイの外部と内部の両方に AP を持つ場合、**config network ap-discovery nat-ip-only disable** コマンドを入力して、管理 NAT アドレスと管理内部アドレスの両方を送信します。AP が取り残されないように、**config ap link-latency disable all** コマンドを必ず入力してください。

次に、AP ディスカバリ応答で NAT IP を有効にする例を示します。

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-fallback

Cisco Lightweight アクセス ポイントのフォールバックを設定するには、**config network ap-fallback** コマンドを使用します。

config network ap-fallback {**enable** | **disable**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのフォール バックをイネーブルにします。
disable	Cisco Lightweight アクセス ポイントのフォール バックをディセーブルにします。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのフォール バックは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Lightweight アクセス ポイントのフォール バックを有効にする例を示します。

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

Lightweight アクセス ポイントを優先するオプションを有効または無効にして、コントローラ障害後にコントローラが先着順ではなく優先順位によって再認証されるようにするには、**config network ap-priority** コマンドを使用します。

config network ap-priority {**enable** | **disable**}

構文の説明

enable	Lightweight アクセス ポイントの優先順位による再認証をイネーブルにします。
disable	Lightweight アクセス ポイントの優先順位による再認証をディセーブルにします。

コマンド デフォルト

Lightweight アクセス ポイントの優先順位による再認証は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Lightweight アクセス ポイントの優先順位による再認証を有効にする例を示します。

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

AppleTalk ブリッジを設定するには、**config network apple-talk** コマンドを使用します。

config network apple-talk {**enable** | **disable**}

構文の説明

enable	AppleTalk のブリッジをイネーブルにします。
disable	AppleTalk のブリッジをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、AppleTalk のブリッジを設定する例を示します。

```
(Cisco Controller) > config network apple-talk enable
```

config network arptimeout

Address Resolution Protocol（ARP）エントリのタイムアウト値を設定するには、**config network arptimeout** コマンドを使用します。

config network arptimeout *seconds*

構文の説明

seconds	秒単位のタイムアウト値です。最小値は10秒です。デフォルト値は 300 秒です。

コマンド デフォルト

デフォルトの ARP エントリ タイムアウト値は 300 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ARP エントリのタイムアウト値を 240 秒に設定する例を示します。

```
(Cisco Controller) > config network arptimeout 240
```

関連コマンド

show network summary

config assisted-roaming

コントローラ上に経由ローミング パラメータを設定するには、**config assisted-roaming** コマンドを使用します。

config assisted-roaming {**denial-maximum** *count* | **floor-bias** *RSSI* | **prediction-minimum** *number_of_APs*}

構文の説明

denial-maximum	アソシエーション拒否の最大カウントを設定します。
count	アクセス ポイントに送信されたアソシエーション リクエストが予測リストのどのアクセス ポイントにも一致しない場合に、クライアントがアソシエーションに拒否される最大回数。値の範囲は 1 ～ 10 です。
floor-bias	同一フロア上のアクセス ポイントに RSSI バイアスを設定します。
RSSI	同一フロア上のアクセス ポイントに対する RSSI バイアス。範囲は 5 ～ 25 です。同一フロア上のアクセス ポイントにはより多くのプリファレンスがあります。
prediction-minimum	経由ローミング機能向けに最適化されたアクセス ポイントの最小数を設定します。
number_of_APs	経由ローミング機能向けに最適化されたアクセス ポイントの最小数。指定できる範囲は1～6です。クライアントに割り当てられた予測のアクセス ポイント数がこの値より小さい場合、経由ローミングは機能しません。

コマンド デフォルト

同一フロア上のアクセス ポイントのデフォルト RSSI バイアスは 15 dBm です。

使用上のガイドライン

802.11k では、クライアントはサービス セットの遷移に使用できる、既知のネイバー アクセス ポイントに関する情報を含むネイバー レポートを要求できるようになります。ネイバー リストによって、アクティブ スキャンおよびパッシブ スキャンを行う必要性が低減されます。

次に、経由ローミング機能向けに最適化されたアクセス ポイントの最小数を設定する例を示します。

```
(Cisco Controller) >config assisted-roaming prediction-minimum 4
```

config network bridging-shared-secret

ブリッジの共有キーを設定するには、**config network bridging-shared-secret** コマンドを使用します。

config network bridging-shared-secret *shared_secret*

構文の説明

shared_secret	ブリッジの共有キーの文字列。文字列には 10 バイトまで使用できます。

コマンド デフォルト

ブリッジの共有キーは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、スイッチに接続するメッシュ アクセス ポイントのバックホール ユーザ データを暗号化する共有キーが作成されます。

このコマンドを機能させるには、zero touch configuration をイネーブルにしておく必要があります。

次に、ブリッジの共有キーの文字列「shhh1」を設定する例を示します。

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

関連コマンド

show network summary

config network broadcast

ブロードキャスト パケット転送を有効または無効にするには、**config network broadcast** コマンドを使用します。

config network broadcast {**enable** | **disable**}

構文の説明

enable	ブロードキャスト パケットの転送をイネーブルにします。
disable	ブロードキャスト パケットの転送をディセーブルにします。

コマンド デフォルト

ブロードキャスト パケットの転送は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用すると、ブロードキャストをイネーブルまたはディセーブルにすることができます。ブロードキャスト転送をイネーブルにする前に、マルチキャスト モードをイネーブルにする必要があります。**config network multicast mode command** コマンドを使用して、コントローラにマルチキャスト モードを設定します。

（注） デフォルトのマルチキャスト モードは、すべてのコントローラの場合はユニキャストです。ブロードキャスト パケットおよびマルチキャスト パケットは個別に制御できます。マルチキャストがオフになり、ブロードキャストがオンになっても、ブロードキャスト パケットは設定されたマルチキャスト モードに基づいてアクセス ポイントに到達します。

次に、ブロードキャスト パケットの転送を有効にする例を示します。

```
(Cisco Controller) > config network broadcast enable
```

関連コマンド

show network summary

config network multicast global

config network multicast mode

config network fast-ssid-change

モバイル端末で高速サービス セット ID（SSID）の変更を有効または無効にするには、**config network fast-ssid-change** コマンドを使用します。

config network fast-ssid-change {**enable** | **disable**}

構文の説明

enable	モバイル ステーションに対して、高速 SSID の変更をイネーブルにします
disable	モバイル ステーションに対して、高速 SSID の変更をディセーブルにします

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

高速 SSID 変更機能を有効にすると、クライアントは SSID 間を移動できます。クライアントが異なる SSID の新しいアソシエーションを送信すると、コントローラの通信テーブルのクライアント エントリがクリアされてから、新しい SSID にクライアントが追加されます。

高速 SSID 変更機能を無効にすると、コントローラによる強制遅延後にクライアントが新しい SSID に移動できます。

次に、モバイル ステーションに対して、高速 SSID の変更を有効にする例を示します。

```
(Cisco Controller) > config network fast-ssid-change enable
```

関連コマンド

show network summary

config network ip-mac-binding

クライアント パケット内での送信元 IP アドレスと MAC アドレスのバインディングを検証するには、**config network ip-mac-binding** コマンドを使用します。

config network ip-network-binding {**enable** | **disable**}

構文の説明

enable	クライアント パケット内での送信元IPアドレスのMACアドレスへのバインディングの検証を有効にします。
disable	クライアント パケット内での送信元IPアドレスのMACアドレスへのバインディングの検証を無効にします。

コマンド デフォルト

クライアント パケット内での送信元 IP アドレスの MAC アドレスへのバインディングの検証は、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

コントローラ ソフトウェア リリース 5.2 では、コントローラがクライアント パケット内の IP アドレスと MAC アドレスとの厳密なバインディングを行います。コントローラは、パケット内のIPアドレスおよびMACアドレスを確認し、これらのアドレスとコントローラに登録されているアドレスを比較します。パケットは、両方が一致した場合に限り転送されます。以前のリリースでは、クライアントの MAC アドレスだけが確認され、IP アドレスは無視されていました。

（注） Workgroup Bridge（WGB）の背後にルーテッド ネットワークが存在する場合は、このバインディング チェックを無効にすることを推奨します。

次に、クライアント パケット内の送信元 IP アドレスと MAC アドレスを検証する例を示します。

```
(Cisco Controller) > config network ip-mac-binding enable
```

config network link local bridging

ローカルサイトでリンク ローカル トラフィックのブリッジングを設定するには、**config network link-local-bridging** コマンドを使用します。

config network link-local-bridging {**enable** | **disable**}

構文の説明

enable	ローカルサイトでリンク ローカル トラフィックのブリッジングを有効にします。
disable	ローカルサイトでリンク ローカル トラフィックのブリッジングを無効にします。

コマンド デフォルト

無効

コマンド履歴

リリース	変更内容
8.0	このコマンドが追加されました。

config network master-base

Cisco ワイヤレス LAN コントローラをアクセス ポイントのデフォルト マスターとして有効または無効にするには、**config network master-base** コマンドを使用します。

config network master-base {**enable** | **disable**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのデフォルト マスターとして機能している Cisco ワイヤレス LAN コントローラをイネーブルにします。
disable	Cisco Lightweight アクセス ポイントのデフォルト マスターとして機能している Cisco ワイヤレス LAN コントローラをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この設定はネットワークのインストール時にのみ使用され、初期ネットワーク設定後は無効にする必要があります。通常、マスター Cisco ワイヤレス LAN コントローラは展開済みネットワークでは使用されないため、マスター Cisco ワイヤレス LAN コントローラの設定は 6.0.199.0 以降のリリースから保存できます。

次に、デフォルト マスターとして Cisco ワイヤレス LAN コントローラを有効にする例を示します。

```
(Cisco Controller) > config network master-base enable
```

config network mgmt-via-wireless

関連付けられている無線クライアントから Cisco ワイヤレス LAN コントローラを管理できるようにするには、**config network mgmt-via-wireless** コマンドを使用します。

config network mgmt-via-wireless {**enable** | **disable**}

構文の説明

enable	ワイヤレス インターフェイスからスイッチ管理をイネーブルにします。
disable	ワイヤレス インターフェイスからスイッチ管理をディセーブルにします。

コマンド デフォルト

ワイヤレス インターフェイスからのスイッチ管理は、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この機能を使用して無線クライアントが管理できるのは、そのクライアントに関連付けられた Cisco ワイヤレス LAN コントローラと、関連付けられた Cisco Lightweight アクセス ポイントのみです。つまり、関連付けられていない他の Cisco ワイヤレス LAN コントローラは管理できません。

次に、ワイヤレス インターフェイスからスイッチ管理を設定する例を示します。

```
(Cisco Controller) > config network mgmt-via-wireless enable
```

関連コマンド

show network summary

config network multicast global

コントローラでマルチキャストを有効または無効にするには、**config network multicast global** コマンドを使用します。

config network multicast global {**enable** | **disable**}

構文の説明

enable	マルチキャスト グローバル サポートをイネーブルにします。
disable	マルチキャスト グローバル サポートをディセーブルにします。

コマンド デフォルト

コントローラでのマルチキャストは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config network broadcast {**enable** | **disable**} コマンドを使用すると、マルチキャスティングを有効または無効にすることなく、ブロードキャスティングを有効または無効にすることができます。このコマンドは、（**config network multicast mode command)** コマンド）を使用して操作するコントローラに設定されたマルチキャスト モードを使用します。

次に、グローバルなマルチキャスト サポートを有効にする例を示します。

```
(Cisco Controller) > config network multicast global enable
```

関連コマンド

show network summary

config network broadcast

config network multicast mode

config network multicast igmp query interval

IGMP クエリー間隔を設定するには、**config network multicast igmp query interval** コマンドを使用します。

config network multicast igmp query interval *value*

構文の説明

value	コントローラが IGMP クエリー メッセージを送信する頻度。範囲は 15 ～ 2400 秒です。

コマンド デフォルト

デフォルトの IGMP クエリー間隔は 20 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

IGMP クエリー間隔を設定するには、次の手順を実行します。

- **config network multicast global enable** コマンドを入力して、グローバル マルチキャストを有効にします。
- **config network multicast igmp snooping enable** コマンドを入力して、IGMP スヌーピングを有効にします。

次に、IGMP クエリー間隔を設定 20 秒に設定する例を示します。

```
(Cisco Controller) > config network multicast igmp query interval 20
```

関連コマンド

config network multicast global

config network multicast igmp snooping

config network multicast igmp timeout

config network multicast igmp snooping

IGMP スヌーピングを有効または無効にするには、**config network multicast igmp snooping** コマンドを使用します。

config network multicast igmp snooping {**enable** | **disable**}

構文の説明

enable	IGMP スヌーピングをイネーブルにします。
disable	IGMP スヌーピングをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、インターネットの IGMP スヌーピング設定を有効にする例を示します。

```
(Cisco Controller) > config network multicast igmp snooping enable
```

関連コマンド

config network multicast global

config network multicast igmp query interval

config network multicast igmp timeout

config network multicast igmp timeout

IGMP タイムアウト値を設定するには、**config network multicast igmp timeout** コマンドを使用します。

config network multicast igmp timeout *value*

構文の説明

value	30 ～ 7200 秒のタイムアウトの範囲。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

timeout には、30 ～ 7200 秒の値を入力できます。特定のマルチキャスト グループに対してクライアントが存在するかどうかを確認するために、コントローラから、1 つのタイムアウト値につき 3 つのクエリが timeout/3 の間隔で送信されます。クライアントから、IGMP レポートを通じて応答を受け取らなかった場合、コントローラはこのクライアントのエントリを MGID テーブルからタイムアウトします。特定のマルチキャスト グループに対するクライアントが残されていない場合、クライアントは IGMP タイムアウト値が経過するまで待ってから、コントローラから MGID エントリを削除します。このコントローラは（宛先アドレス 224.0.0.1 に対して）常に一般的な IGMP クエリーを生成し、MGID 値が 1 である WLAN すべてに送信します。

次に、IGMP ネットワーク設定のタイムアウト値 50 を設定する例を示します。

```
(Cisco Controller) > config network multicast igmp timeout 50
```

関連コマンド

config network multicast global

config network igmp snooping

config network multicast igmp query interval

config network multicast l2mcast

1 つのインターフェイスまたはすべてのインターフェイスにレイヤ 2 マルチキャストを設定するには、**config network multicast l2mcast** コマンドを使用します。

config network multicast l2mcast {**enable** | **disable** {**all** | *interface-name*}

構文の説明

enable	レイヤ 2 マルチキャストをイネーブルにします。
disable	レイヤ 2 マルチキャストをディセーブルにします。
all	すべてのインターフェイスに適用します。
interface-name	レイヤ 2 マルチキャストがイネーブルまたはディセーブルにされたインターフェイス名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのインターフェイスに対してレイヤ 2 マルチキャストを有効にする例を示します。

```
(Cisco Controller) > config network multicast l2mcast enable all
```

関連コマンド

config network multicast global

config network multicast igmp snooping

config network multicast igmp query interval

config network multicast mld

config network multicast mld

Multicast Listener Discovery（MLD）パラメータを設定するには、**config network multicast mld** コマンドを使用します。

config network multicast mld {**query interval** *interval-value* | **snooping** {**enable** | **disable**} | **timeout** *timeout-value*}

構文の説明

query interval	MLD クエリー メッセージを送信するようにクエリー間隔を設定します。
interval-value	秒単位のクエリー間隔です。範囲は 15 ～ 2400 秒です。
snooping	MLD スヌーピングを設定します。
enable	MLD スヌーピングをイネーブルにします。
disable	MLD スヌーピングをディセーブルにします。
timeout	MLD のタイムアウトを設定します。
timeout-value	秒単位のタイムアウト値です。範囲は 30 ～ 7200 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MLD クエリー メッセージに 20 秒のクエリー間隔を設定する例を示します。

```
(Cisco Controller) > config network multicast mld query interval 20
```

関連コマンド

config network multicast global

config network multicast igmp snooping

config network multicast igmp query interval

config network multicast l2mcast

config network multicast mode multicast

ブロードキャストパケットまたはマルチキャストパケットをアクセスポイントに送信する際、マルチキャスト方式を使用するようにコントローラを設定するには、**config network multicast mode multicast** コマンドを使用します。

config network multicast mode multicast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、マルチキャスト レシーバにデータのコピーを 1 つ送信するマルチキャスト モードを設定する例を示します。

```
(Cisco Controller) > config network multicast mode multicast
```

関連コマンド

config network multicast global

config network broadcast

config network multicast mode unicast

config network multicast mode unicast

ブロードキャストパケットまたはマルチキャストパケットをアクセスポイントに送信する際、ユニキャスト方式を使用するようにコントローラを設定するには、**config network multicast mode unicast** コマンドを使用します。

config network multicast mode unicast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラがユニキャスト モードを使用するように設定する例を示します。

```
(Cisco Controller) > config network multicast mode unicast
```

関連コマンド

config network multicast global

config network broadcast

config network multicast mode multicast

config network oeap-600 dual-rlan-ports

Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、ポート 4 に加えて、リモート LAN ポートとしても機能するように設定するには、**config network oeap-600 dual-rlan-ports** コマンドを使用します。

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

構文の説明

enable	Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、ポート 4 に加えて、リモート LAN ポートとしても機能できるようにします。
disable	Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネットポート3をリセットして、ローカル LAN ポートとして機能するようにします。

コマンド デフォルト

Cisco 600 シリーズ OEAP のイーサネット ポート 3 がリセットされます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、リモートの LAN ポートとして機能できるようにする例を示します。

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network oeap-600 local-network

Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスを設定するには、**config network oeap-600 local-network** コマンドを使用します。

config network oeap-600 local-network {**enable** | **disable**}

構文の説明

enable	Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスをイネーブルにします。
disable	Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスをディセーブルにします。

コマンド デフォルト

Cisco 600 シリーズ OEAP のローカル ネットワークへのアクセスは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスを有効にする例を示します。

```
(Cisco Controller) > config network oeap-600 local-network enable
```

config network otap-mode

Cisco Lightweight アクセス ポイントの無線プロビジョニング（OTAP）を有効または無効にするには、**config network otap-mode** コマンドを使用します。

config network otap-mode {**enable** | **disable**}

構文の説明

enable	OTAP プロビジョニングをイネーブルにします。
disable	OTAP プロビジョニングをディセーブルにします。

コマンド デフォルト

OTAP プロビジョニングは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、OTAP プロビジョニングを無効にする例を示します。

```
(Cisco Controller) >config network otap-mode disable
```

config network profiling

特定のポートの HTTP ポートをプロファイルするには、**config network profiling http-port** コマンドを使用します。

config network profiling http-port ポート番号

構文の説明

ポート番号	インターフェイス ポート番号。デフォルト値は 80 です。

コマンド履歴

リリース	変更内容
8.2	このコマンドが追加されました。

次に、ネットワークの HTTP ポートを設定する例を示します。

```
(Cisco Controller) > config network profiling http-port 80
```

config pmipv6 domain

PMIPv6 を設定し、Cisco のモバイル アクセス ゲートウェイ（MAG）機能を有効にするには、**config pmipv6 domain** コマンドを使用します。

config pmipv6 domain *domain_name*

構文の説明

domain_name	PMIPv6 ドメインの名前。ドメイン名は最大 127 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、PMIPv6 WLAN のドメイン名を設定する例を示します。

```
(Cisco Controller) >config pmipv6 domain floor1
```

config pmipv6 add profile

WLAN のプロキシ モビリティ IPv6（PMIPv6）プロファイルを作成するには、**config pmipv6 add profile** コマンドを使用します。レルムまたは Service Set Identifier（SSID）に基づいて、PMIPv6 プロファイルを設定できます。

config pmipv6 add profile *profile_name* **nai** {*user@realm* | *@realm* | *****} **lma** *lma_name* **apn** *apn_name*

構文の説明

profile_name	プロファイルの名前プロファイル名は最大 127 文字の英数字で、大文字と小文字を区別します。
nai	クライアントのネットワーク アクセス ID を指定します。
user@realm	*user*@realm 形式のクライアントのネットワーク アクセス ID。NAI 名は最大 127 文字の英数字で、大文字と小文字を区別します。
@realm	@realm 形式のクライアントのネットワーク アクセス ID。
*	すべてのネットワーク アクセス ID。すべてのユーザに対して、SSID に基づいてプロファイルを用意できます。
lma	Local Mobility Anchor（LMA）を指定します。
lma_name	LMA の名前。LMA 名は最大 127 文字の英数字で、大文字と小文字を区別します。
apn	アクセス ポイントを指定します。
ap_name	アクセス ポイントの名前。アクセス ポイント名は最大 127 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラがオープン認証を使用する場合、このコマンドは、PMIPv6 コンフィギュレーション コマンドを使用するための前提条件です。

次に、PMIPv6 プロファイルを作成する例を示します。

```
(Cisco Controller) >config pmipv6 add profile profile1 nai @vodfone.com lma vodfonelma apn vodafoneapn
```

config pmipv6 delete

プロキシ モビリティ IPv6（PMIPv6）プロファイル、ドメイン、または Local Mobility Anchor（LMA）を削除するには、 **config pmipv6 delete** コマンドを使用します。

config pmipv6 delete {**profile** *profile_name* **nai** { *nai_id* | **all** } | **domain** *domain_name* | **lma** *lma_name*}

構文の説明

profile	PMIPv6 プロファイルを指定します。
profile_name	PMIPv6 プロファイルの名前。プロファイル名は最大 127 文字の英数字で、大文字と小文字を区別します。
nai	モバイル クライアントのネットワーク アクセス ID（NAI）を指定します。
nai_id	モバイル クライアントのネットワーク アクセス ID。NAI は最大 127 文字の英数字で、大文字と小文字を区別します。
all	すべての NAI を指定します。すべての NAI を削除すると、プロファイルが削除されます。
domain	PMIPv6 ドメインを指定します。
domain_name	PMIPv6 ドメインの名前。ドメイン名は最大 127 文字の英数字で、大文字と小文字を区別します。
lma	LMA を指定します。
lma_name	LMA の名前。LMA 名は最大 127 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ドメインを削除する例を示します。

```
(Cisco Controller) >config pmipv6 delete lab1
```

config pmipv6 mag apn

モバイル アクセス ゲートウェイ（MAG）のアクセス ポイント名（APN）を設定するには、**config pmipv6 mag apn** コマンドを使用します。

config pmipv6 mag apn *apn-name*

構文の説明

apn-name	MAGのアクセスポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、MAG ロールは WLAN です。ただし Lightweight アクセス ポイントの場合、MAG ロールは 3GPP に設定する必要があります。MAG ロールが 3GPP の場合、MAG の APN を指定する必要があります。

MAG の APN を削除するには、**config pmipv6 delete mag apn** *apn-name* コマンドを使用します。

次に、MAG の APN を追加する例を示します。

```
(Cisco Controller) >config pmipv6 mag apn myCiscoAP
```

config pmipv6 mag binding init-retx-time

モバイル アクセス ゲートウェイ（MAG）がプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の初期タイムアウトを設定するには、 **config pmipv6 mag binding init-retx-time** コマンドを使用します。

config pmipv6 mag binding init-retx-time *units*

構文の説明

units	MAG が PBA を受信しない場合の PBU 間の初期タイムアウト。範囲は 100 ～ 65535 秒です。

コマンド デフォルト

デフォルトの初期タイムアウトは 1000 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAG が PBA を受信しない場合に PBU 間の初期タイムアウトを設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding init-retx-time 500
```

config pmipv6 mag binding lifetime

モバイルアクセス ゲートウェイ（MAG）のバインディング エントリのライフタイムを設定するには、 **config pmipv6 mag binding lifetime** コマンドを使用します。

config pmipv6 mag binding lifetime *units*

構文の説明

units	MAG のバインディング エントリのライフタイム。バインディング ライフタイムは 4 秒の倍数であることが必要です。範囲は 10 ～ 65535 秒です。

コマンド デフォルト

バインディング エントリのデフォルトのライフタイムは 65535 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラのバインディング エントリのライフタイムを設定する前に、プロキシモビリティ IPv6（PMIPv6）ドメインを設定する必要があります。

次に、コントローラのバインディング エントリのライフタイムを設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding lifetime 5000
```

config pmipv6 mag binding max-retx-time

モビリティ アクセス ゲートウェイ（MAG）がプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の最大タイムアウトを設定するには、 **config pmipv6 mag binding max-retx-time** コマンドを使用します。

config pmipv6 mag binding max-retx-time *units*

構文の説明

units	MAG が PBA を受信しない場合の PBU 間の最大タイムアウト。範囲は 100 ～ 65535 秒です。

コマンド デフォルト

デフォルトの最大タイムアウトは 32000 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAG が PBA を受信しない場合の PBU 間の最大タイムアウトを設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding max-retx-time 50
```

config pmipv6 mag binding maximum

モバイル アクセス ゲートウェイ（MAG）のバインディング エントリの最大数を設定するには、 **config pmipv6 mag binding maximum** コマンドを使用します。

config pmipv6 mag binding maximum *units*

構文の説明

units	MAG のバインディング エントリの最大数。この番号は、MAG に接続されるユーザの最大数を示します。範囲は 0 ～ 40000 です。

コマンド デフォルト

MAG のバインディング エントリのデフォルトの最大数は 10000 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

MAG のバインディング エントリの最大数を設定する前に、プロキシモビリティ IPv6（PMIPv6）ドメインを設定する必要があります。

次に、MAG のバインディング エントリの最大数を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding maximum 20000
```

config pmipv6 mag binding refresh-time

MAG のバインディング エントリのリフレッシュ時間を設定するには、 **config pmipv6 mag binding refresh-time** コマンドを使用します。

config pmipv6 mag binding refresh-time *units*

構文の説明

units	MAGのバインディングエントリのリフレッシュ時間。バインディングのリフレッシュ時間は、4 の倍数である必要があります。範囲は 4 ～ 65535 秒です。

コマンド デフォルト

MAG のバインディング エントリのリフレッシュ時間は、デフォルトでは 300 秒です。

使用上のガイドライン

MAG のバインディング エントリのリフレッシュ時間を設定する前に、PMIPv6 ドメインを設定する必要があります。

次に、MAGのバインディングエントリのリフレッシュ時間を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag binding refresh-time 500
```

config pmipv6 mag bri delay

MAG が Binding Revocation Indication（BRI）メッセージを再送信するまでに待機する最大時間または最小時間を設定するには、 **config pmipv6 mag bri delay** コマンドを使用します。

config pmipv6 mag bri delay {**min** | **max**} *time*

構文の説明

min	MAG が BRI メッセージを再送信するまでに待機する最小時間を指定します。
max	MAG が BRI メッセージを再送信するまでに待機する最大時間を指定します。
time	Cisco WLC が BRI メッセージを再送信するまでに待機する最大時間または最小時間。指定できる範囲は 500 ～ 65535 ミリ秒です。

コマンド デフォルト

MAG が BRI メッセージを再送信するまでに待機する最大時間のデフォルト値は 2 秒です。

MAG が BRI メッセージを再送信するまでに待機する最小時間のデフォルト値は 1 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAG が BRI メッセージを再送信するまでに待機する最大時間を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag bri delay min 500
```

config pmipv6 mag bri retries

MAG が Binding Revocation Acknowledgement（BRA）メッセージを受信する前に Binding Revocation Indication（BRI）メッセージを再送信する最大回数を設定するには、 **config pmipv6 mag bri retries** コマンドを使用します。

config pmipv6 mag bri retries *retries*

構文の説明

retries	MAG が BRA メッセージを受信する前に BRI メッセージを再送信する最大回数。指定できる範囲は 1 ー 10 回です。

コマンド デフォルト

デフォルトは 1 回です。

次に、MAG が再試行する最大回数を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag bri retries 5
```

config pmipv6 mag lma

モバイル アクセス ゲートウェイ（MAG）でローカル モビリティ アンカー（LMA）を設定するには、 **config pmipv6 mag lma** コマンドを使用します。

config pmipv6 mag lma *lma_name* **ipv4-address** *address*

構文の説明

lma_name	LMA の名前。LMA 名は、LMA を一意に識別する NAI または文字列にすることができます。
ipv4-address	LMA の IP アドレスを指定します。
address	LMA の IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、MAG で PMIPv6 のパラメータを設定するための前提条件です。

次に、MAG で LMA を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag lma vodafonelma ipv4-address 209.165.200.254
```

config pmipv6 mag replay-protection

リプレイ保護のために、受信したプロキシバインディング確認（PBA）のタイムスタンプと現在の日時との最大時間差を設定するには、 **config pmipv6 mag replay-protection** コマンドを使用します。

config pmipv6 mag replay-protection { **timestamp window** *time* | **sequence-no** *sequence* | **mobile-node-timestamp** *mobile_node_timestamp* }

構文の説明

timestamp	PBA メッセージのタイムスタンプを指定します。
window	受信した PBA メッセージのタイムスタンプと現在時刻間の最大時間差を指定します。
time	受信した PBA メッセージのタイムスタンプと現在時刻間の最大時間差。範囲は 1 ～ 300 ミリ秒です。
sequence-no	（任意）Proxy Binding Update メッセージのシーケンス番号を指定します。
sequence	（任意）Proxy Binding Update メッセージのシーケンス番号。
mobile_node_timestamp	（任意）モバイルノードのタイムスタンプを指定します。
mobile_node_timestamp	（任意）モバイル ノードのタイムスタンプ。

コマンド デフォルト

デフォルトの最大時間差は 300 ミリ秒です。

使用上のガイドライン

タイムスタンプ オプションだけがサポートされています。

次に、受信したPBAメッセージのタイムスタンプと現在時刻間の最大時間差（ミリ秒単位）を設定する例を示します。

```
(Cisco Controller) >config pmipv6 mag replay-protection timestamp window 200
```

config port power

特定のコントローラ ポートまたはすべてのポートの Power over Ethernet（PoE）を有効または無効にするには、**config port power** コマンドを使用します。

config port power {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのポートで PoE を有効にする例を示します。

```
(Cisco Controller) > config port power all enable
```

次に、ポート 8 で PoE を無効にする例を示します。

```
(Cisco Controller) > config port power 8 disable
```

config network rf-network-name

RF ネットワーク名を設定するには、**config network rf-network-name** コマンドを使用します。

config network rf-network-name *name*

構文の説明

name	RF ネットワーク名。名前には最大 19 文字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、旅行者に RF ネットワーク名を設定する例を示します。

```
(Cisco Controller) > config network rf-network-name travelers
```

関連コマンド

show network summary

config network secureweb

管理ユーザのセキュア Web（https は http および SSL）インターフェイスの状態を変更するには、**config network secureweb** コマンドを使用します。

config network secureweb {**enable** | **disable**}

構文の説明

enable	管理ユーザのセキュア Web インターフェイスをイネーブルにします。
disable	管理ユーザのセキュア Web インターフェイスをディセーブルにします。

コマンド デフォルト

管理ユーザのセキュア Web インターフェイスは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、管理ユーザは http://ip-address を使用してコントローラの GUI にアクセスできるようになります。Web モードの接続は、セキュリティで保護されません。

次に、管理ユーザのセキュア Web インターフェイス設定を有効にする例を示します。

```
(Cisco Controller) > config network secureweb enable
You must reboot for the change to take effect.
```

関連コマンド

config network secureweb cipher-option

show network summary

config network secureweb cipher-option

セキュリティを強化したセキュアWebモードを有効または無効にするか、Web管理およびWeb認証用のセキュア ソケット レイヤ（SSL v2）を有効または無効にするには、**config network secureweb cipher-option** コマンドを使用します。

config network secureweb cipher-option {**high** | **sslv2** | **rc4-preference**} {**enable** | **disable**}

構文の説明

high	Web 管理および Web 認証に 128 ビット暗号化が必要であるかどうかを設定します。
sslv2	Web 管理と Web 認証の両方に対して SSLv2 を設定します。
rc4-preference	Web 管理と Web 認証に関して、RC4-SHA（Rivest Cipher 4 セキュア ハッシュ アルゴリズム）暗号スイートを優先するように設定します。
enable	セキュア Web インターフェイスをイネーブルにします。
disable	セキュア Web インターフェイスをディセーブルにします。

コマンド デフォルト

セキュリティが強化されたセキュア Web モードの場合はデフォルトで **disable** であり、SSL v2 の場合は **enable** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

（注） **config network secureweb cipher-option** コマンドを使用すると、http://ip-address を使用してコントローラ GUI にアクセスできるようになります。ただし、このアクセスは 128 ビット以上の暗号方式をサポートしているブラウザからに限り可能です。

cipher-option sslv2 が無効の場合、SSLv2 だけで設定されているブラウザを使用して接続することはできません。SSLv3 以降などセキュリティの強化されたプロトコルを使用するように設定されたブラウザを使用する必要があります。

RC4-SHA ベースの暗号スイートでは、RC4 が暗号化に使用され、SHA はメッセージ認証に使用されます。

次に、セキュリティが強化されたセキュア Web モードを有効にする例を示します。

```
(Cisco Controller) > config network secureweb cipher-option
```

次に、SSL V2 を無効にする例を示します。

```
(Cisco Controller) > config network secureweb cipher-option sslv2 disable
```

関連コマンド

config network secureweb

show network summary

config network ssh

新規セキュア シェル（SSH）セッションを有効または無効にするには、**config network ssh** コマンドを使用します。

config network ssh {**enable** | **disable**}

構文の説明

enable	新規 SSH セッションを許可します。
disable	新規 SSH セッションを拒否します。

コマンド デフォルト

新しい SSH セッションのデフォルト値は **disable** です。

次に、新規 SSH セッションを有効にする例を示します。

```
(Cisco Controller) > config network ssh enable
```

関連コマンド

show network summary

config network telnet

新規 Telnet セッションを許可または拒否するには、**config network telnet** コマンドを使用します

config network telnet {**enable** | **disable**}

構文の説明

enable	新規 Telnet セッションを許可します。
disable	新規 Telnet セッションを拒否します。

コマンド デフォルト

デフォルトでは、新規 Telnet セッションは拒否され、値は **disable** です。

使用上のガイドライン

Telnet は、Cisco Aironet 1830 および 1850 シリーズ アクセス ポイントではサポートされていません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、新規 Telnet セッションを設定する例を示します。

```
(Cisco Controller) > config network telnet enable
```

関連コマンド

config ap telnet

show network summary

config network usertimeout

アイドル状態のクライアント セッションのタイムアウトを変更するには、**config network usertimeout** コマンドを使用します。

config network usertimeout *seconds*

構文の説明

seconds	タイムアウト時間（秒）。最小値は 90 秒です。デフォルト値は 300 秒です。

コマンド デフォルト

アイドル状態のクライアント セッションのデフォルト タイムアウト値は 300 秒です。

使用上のガイドライン

このコマンドを使用して、Cisco ワイヤレス LAN コントローラ上のアイドル状態のクライアント セッション時間を設定します。最小時間は 90 秒です。

次に、アイドル セッション タイムアウトを 1200 秒に設定する例を示します。

```
(Cisco Controller) > config network usertimeout 1200
```

関連コマンド

show network summary

config network web-auth captive-bypass

ネットワーク レベルでキャプティブ ポータルのバイパスをサポートするようにコントローラを設定するには、**config network web-auth captive-bypass** コマンドを使用します。

config network web-auth captive-bypass {**enable** | **disable**}

構文の説明

enable	コントローラがキャプティブ ポータルのバイパスをサポートできるようにします。
disable	コントローラがキャプティブ ポータルのバイパスをサポートできないようにします。

コマンド デフォルト

なし

次に、キャプティブ ポータルのバイパスをサポートするようにコントローラを設定する例を示します。

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

関連コマンド

show network summary

config network web-auth cmcc-support

config network web-auth cmcc-support

コントローラで eWalk を設定するには、**config network web-auth cmcc-support** コマンドを使用します。

config network web-auth cmcc-support {**enable** | **disable**}

構文の説明

enable	コントローラの eWalk をイネーブルにします。
disable	コントローラの eWalk をディセーブルにします。

コマンド デフォルト

なし

次に、コントローラの eWalk を有効にする例を示します。

```
(Cisco Controller) > config network web-auth cmcc-support enable
```

関連コマンド

show network summary

config network web-auth captive-bypass

config network web-auth port

ネットワーク レベルの Web 認証に関して追加ポートがリダイレクトされるように設定するには、**config network web-auth port** コマンドを使用します。

config network web-auth port *port*

構文の説明

port	ポート番号。有効な範囲は 0 ～ 65535 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web認証に関して、追加ポート番号1200がリダイレクトされるように設定する例を示します。

```
(Cisco Controller) > config network web-auth port 1200
```

関連コマンド

show network summary

config network web-auth proxy-redirect

Web認証クライアントのプロキシのリダイレクションサポートを設定するには、**config network web-auth proxy-redirect** コマンドを使用します。

config network web-auth proxy-redirect {**enable** | **disable**}

構文の説明

enable	Web 認証クライアントのプロキシ リダイレクションをサポートできるようにします。
disable	Web 認証クライアントのプロキシ リダイレクションをサポートできないようにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

関連コマンド

show network summary

config network web-auth secureweb

クライアントにセキュア Web（https）認証を設定するには、**config network web-auth secureweb** コマンドを使用します。

config network web-auth secureweb {**enable** | **disable**}

構文の説明

enable	クライアントにセキュア Web（https）認証を行えるようにします。
disable	クライアントにセキュア Web（https）認証を行えないようにします。クライアントのHTTP Web 認証を有効にします。

コマンド デフォルト

デフォルトでは、クライアントのセキュア Web（https）認証は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

config network web-auth secureweb disable コマンドを使用してクライアントのセキュア Web（https）認証を設定する場合、Cisco WLC をリブートして変更を適用する必要があります。

次に、クライアントに対してセキュア Web（https）認証を有効にする例を示します。

```
(Cisco Controller) > config network web-auth secureweb enable
```

関連コマンド

show network summary

config network web-auth https-redirect

Web 認証クライアントの HTTPS リダイレクション サポートを設定するには、**config network web-auth https-redirect** コマンドを使用します。

config network web-auth https-redirect {**enable** | **disable**}

構文の説明

enable	Web 認証クライアントのセキュア リダイレクション（HTTPS）を有効にします。
disable	Web 認証クライアントのセキュア リダイレクション（HTTPS）を無効にします。

コマンド デフォルト

このコマンドは、デフォルトでは無効になっています。

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth https-redirect enable
```

関連コマンド

show network summary

config network webcolor

コントローラ GUI の Web カラー テーマを設定するには、**config network webcolor** コマンドを使用します。

config network webcolor {**default** | **red**}

構文の説明

default	コントローラ GUI のデフォルト Web カラー テーマを指定します。
red	コントローラ GUI の Web カラー テーマを赤に指定します。

コマンド デフォルト

default

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

コントローラ CLI から Web カラー テーマを変更した場合、変更を適用するにはコントローラ GUI をリロードする必要があります。

次に、コントローラ GUI の Web インターフェイスの色を赤に設定する例を示します。

```
(Cisco Controller) > config network webcolor red
```

config network webmode

Web モードを有効または無効にするには、**config network webmode** コマンドを使用します。

config network webmode {**enable** | **disable**}

構文の説明

enable	Webインターフェイスをイネーブルにします。
disable	Web インターフェイスをディセーブルにします。

コマンド デフォルト

Web モードのデフォルト値は **enable** です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web インターフェイス モードを無効にする例を示します。

```
(Cisco Controller) > config network webmode disable
```

関連コマンド

show network summary

config network web-auth

ネットワーク レベルの Web 認証オプションを設定するには、**config network web-auth** コマンドを使用します。

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

構文の説明

port	Web 認証リダイレクション用に追加ポートを設定します。
port-number	ポート番号（0 ～ 65535）。
proxy-redirect	Web 認証クライアントのプロキシ リダイレクション サポートを設定します。
enable	Web 認証クライアントのプロキシ リダイレクション サポートをイネーブルにします。 （注） Web 認証プロキシのリダイレクションは、ポート 80、8080、および 3128 に加え、ユーザ定義のポート 345 に対してイネーブルになります。
disable	Web 認証クライアントのプロキシ リダイレクション サポートをディセーブルにします。

コマンド デフォルト

ネットワーク レベルの Web 認証のデフォルト値は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

設定を有効にするには、システムをリセットする必要があります。

次に、Web 認証クライアントのプロキシのリダイレクションのサポートを有効にする例を示します。

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

関連コマンド

show network summary

show run-config

config qos protocol-type

config network zero-config

ブリッジのアクセス ポイントの ZeroConfig サポートを設定するには、**config network zero-config** コマンドを使用します。

config network zero-config {**enable** | **disable**}

構文の説明

enable	ブリッジのアクセス ポイントの ZeroConfig サポートをイネーブルにします。
disable	ブリッジのアクセス ポイントの ZeroConfig サポートをディセーブルにします。

コマンド デフォルト

ブリッジのアクセス ポイントの ZeroConfig サポートは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ブリッジのアクセス ポイントの ZeroConfig サポートを有効にする例を示します。

```
(Cisco Controller) >config network zero-config enable
```

config network allow-old-bridge-aps

スイッチとアソシエートする古いブリッジ アクセス ポイントの機能を設定するには、**config network allow-old-bridge-aps** コマンドを使用します。

config network allow-old-bridge-aps {**enable** | **disable**}

構文の説明

enable	スイッチ アソシエーションをイネーブルにします。
disable	スイッチ アソシエーションをディセーブルにします。

コマンド デフォルト

スイッチ アソシエーションは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、古いブリッジアクセスポイントをスイッチに関連付けるように設定する例を示します。

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

AP ディスカバリ応答で NAT IP を有効または無効にするには、**config network ap-discovery** コマンドを使用します。

config network ap-discovery nat-ip-only {**enable** | **disable**}

構文の説明

enable	NAT IP の使用をディスカバリ応答でのみイネーブルにします。
disable	ディスカバリ応答での NAT IP および非 NAT IP の両方の使用をイネーブルにします。

コマンド デフォルト

NAT IP の使用がディスカバリ応答でのみ有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config interface nat-address management コマンドが設定されている場合、このコマンドによって、CAPWAP ディスカバリ応答で送信されるアドレスが制御されます。

すべての AP がコントローラの NAT ゲートウェイの外側にある場合、**config network ap-discovery nat-ip-only enable** コマンドを入力して、管理 NAT アドレスのみを送信します。

コントローラが、NAT ゲートウェイの外部と内部の両方に AP を持つ場合、**config network ap-discovery nat-ip-only disable** コマンドを入力して、管理 NAT アドレスと管理内部アドレスの両方を送信します。AP が取り残されないように、**config ap link-latency disable all** コマンドを必ず入力してください。

次に、AP ディスカバリ応答で NAT IP を有効にする例を示します。

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-fallback

Cisco Lightweight アクセス ポイントのフォールバックを設定するには、**config network ap-fallback** コマンドを使用します。

config network ap-fallback {**enable** | **disable**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのフォール バックをイネーブルにします。
disable	Cisco Lightweight アクセス ポイントのフォール バックをディセーブルにします。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのフォール バックは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Lightweight アクセス ポイントのフォール バックを有効にする例を示します。

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

Lightweight アクセス ポイントを優先するオプションを有効または無効にして、コントローラ障害後にコントローラが先着順ではなく優先順位によって再認証されるようにするには、**config network ap-priority** コマンドを使用します。

config network ap-priority {**enable** | **disable**}

構文の説明

enable	Lightweight アクセス ポイントの優先順位による再認証をイネーブルにします。
disable	Lightweight アクセス ポイントの優先順位による再認証をディセーブルにします。

コマンド デフォルト

Lightweight アクセス ポイントの優先順位による再認証は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Lightweight アクセス ポイントの優先順位による再認証を有効にする例を示します。

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

AppleTalk ブリッジを設定するには、**config network apple-talk** コマンドを使用します。

config network apple-talk {**enable** | **disable**}

構文の説明

enable	AppleTalk のブリッジをイネーブルにします。
disable	AppleTalk のブリッジをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、AppleTalk のブリッジを設定する例を示します。

```
(Cisco Controller) > config network apple-talk enable
```

config network bridging-shared-secret

ブリッジの共有キーを設定するには、**config network bridging-shared-secret** コマンドを使用します。

config network bridging-shared-secret *shared_secret*

構文の説明

shared_secret	ブリッジの共有キーの文字列。文字列には 10 バイトまで使用できます。

コマンド デフォルト

ブリッジの共有キーは、デフォルトでは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドにより、スイッチに接続するメッシュ アクセス ポイントのバックホール ユーザ データを暗号化する共有キーが作成されます。

このコマンドを機能させるには、zero touch configuration をイネーブルにしておく必要があります。

次に、ブリッジの共有キーの文字列「shhh1」を設定する例を示します。

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

関連コマンド

show network summary

config network master-base

Cisco ワイヤレス LAN コントローラをアクセス ポイントのデフォルト マスターとして有効または無効にするには、**config network master-base** コマンドを使用します。

config network master-base {**enable** | **disable**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのデフォルト マスターとして機能している Cisco ワイヤレス LAN コントローラをイネーブルにします。
disable	Cisco Lightweight アクセス ポイントのデフォルト マスターとして機能している Cisco ワイヤレス LAN コントローラをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この設定はネットワークのインストール時にのみ使用され、初期ネットワーク設定後は無効にする必要があります。通常、マスター Cisco ワイヤレス LAN コントローラは展開済みネットワークでは使用されないため、マスター Cisco ワイヤレス LAN コントローラの設定は 6.0.199.0 以降のリリースから保存できます。

次に、デフォルト マスターとして Cisco ワイヤレス LAN コントローラを有効にする例を示します。

```
(Cisco Controller) > config network master-base enable
```

config network oeap-600 dual-rlan-ports

Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、ポート 4 に加えて、リモート LAN ポートとしても機能するように設定するには、**config network oeap-600 dual-rlan-ports** コマンドを使用します。

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

構文の説明

enable	Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、ポート 4 に加えて、リモート LAN ポートとしても機能できるようにします。
disable	Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネットポート3をリセットして、ローカル LAN ポートとして機能するようにします。

コマンド デフォルト

Cisco 600 シリーズ OEAP のイーサネット ポート 3 がリセットされます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco OfficeExtend 600 シリーズ アクセス ポイントのイーサネット ポート 3 が、リモートの LAN ポートとして機能できるようにする例を示します。

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network oeap-600 local-network

Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスを設定するには、**config network oeap-600 local-network** コマンドを使用します。

config network oeap-600 local-network {**enable** | **disable**}

構文の説明

enable	Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスをイネーブルにします。
disable	Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスをディセーブルにします。

コマンド デフォルト

Cisco 600 シリーズ OEAP のローカル ネットワークへのアクセスは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco 600 シリーズ OfficeExtend アクセス ポイントのローカル ネットワークへのアクセスを有効にする例を示します。

```
(Cisco Controller) > config network oeap-600 local-network enable
```

config network otap-mode

Cisco Lightweight アクセス ポイントの無線プロビジョニング（OTAP）を有効または無効にするには、**config network otap-mode** コマンドを使用します。

config network otap-mode {**enable** | **disable**}

構文の説明

enable	OTAP プロビジョニングをイネーブルにします。
disable	OTAP プロビジョニングをディセーブルにします。

コマンド デフォルト

OTAP プロビジョニングは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、OTAP プロビジョニングを無効にする例を示します。

```
(Cisco Controller) >config network otap-mode disable
```

config network zero-config

ブリッジのアクセス ポイントの ZeroConfig サポートを設定するには、**config network zero-config** コマンドを使用します。

config network zero-config {**enable** | **disable**}

構文の説明

enable	ブリッジのアクセス ポイントの ZeroConfig サポートをイネーブルにします。
disable	ブリッジのアクセス ポイントの ZeroConfig サポートをディセーブルにします。

コマンド デフォルト

ブリッジのアクセス ポイントの ZeroConfig サポートは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ブリッジのアクセス ポイントの ZeroConfig サポートを有効にする例を示します。

```
(Cisco Controller) >config network zero-config enable
```

config nmsp notify-interval measurement

コントローラの Network Mobility Services Protocol (NMSP) 通知間隔値をネットワーク内の遅延に対応するように変更するには、**config nmsp notify-interval measurement** コマンドを使用します。

config nmsp notify-interval measurement {**client** | **rfid** | **rogue**} *interval*

構文の説明

client	クライアントの間隔を変更します。
rfid	アクティブな無線周波数ID（RFID）タグの間隔を変更します。
rogue	不正なアクセス ポイントおよび不正なクライアントの間隔を変更します。
interval	時間間隔。範囲は 1 ～ 30 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラとロケーション アプライアンスとの通信には、TCP ポート 16113 が使用されます。コントローラとロケーションアプライアンスの間にファイアウォールがある場合は、NMSP が機能するにはこのポートが開いている（ブロックされていない）ことが必要です。

次に、アクティブな RFID タグの NMSP 通知間隔を 25 秒に変更する例を示します。

```
(Cisco Controller) > config nmsp notify-interval measurement rfid 25
```

関連コマンド

clear locp statistics

clear nmsp statistics

show nmsp notify-interval summary

show nmsp statistics

show nmsp status

config paging

ページのスクロールを有効または無効にするには、**config paging** コマンドを使用します。

config paging {**enable** | **disable**}

構文の説明

enable	ページのスクロールをイネーブルにします。
disable	ページのスクロールをディセーブルにします。

コマンド デフォルト

デフォルトでは、ページのスクロールは有効になっています。

使用上のガイドライン

ページのスクロールを無効にした状態で膨大な数の出力行を生成するコマンドを実行すると、SSH/Telnet 接続またはコンソールでのユーザ セッションが終了する可能性があります。

次に、ページのスクロールを有効にする例を示します。

```
(Cisco Controller) > config paging enable
```

関連コマンド

show run-config

config passwd-cleartext

プレーン テキストでのパスワードの一時的な表示を有効または無効にするには、**config passwd-cleartext** コマンドを使用します。

config passwd-cleartext {**enable** | **disable**}

構文の説明

enable	プレーン テキストでのパスワードの表示をイネーブルにします。
disable	プレーンテキストでのパスワードの表示をディセーブルにします。

コマンド デフォルト

デフォルトでは、プレーン テキストでのパスワードの一時的な表示は無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

show run-config コマンドを使用する際にユーザが割り当てたパスワードをクリア テキストで表示する場合には、このコマンドを無効にする必要があります。

このコマンドを実行するには、admin パスワードを入力する必要があります。このコマンドは、この特定のセッションだけで有効です。リブート後には保存されません。

次に、プレーン テキストでパスワードの表示を有効にする例を示します。

```
(Cisco Controller) > config passwd-cleartext enable
The way you see your passwds will be changed
You are being warned.
Enter admin password:
```

関連コマンド

show run-config

config policy

Cisco ワイヤレス LAN コントローラ（WLC）でネイティブ プロファイリング ポリシーを設定するには、**config policy** コマンドを使用します。

config policy*policy_name* {**action** {**acl** {**enable** | **disable**} *acl_name* | {**average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate** | **qos** | **session-timeout** | **sleeping-client-timeout** | **avc-profile-name** {**enable** *avc_profile_name* | **disable**} | **vlan**} {**enable** | **disable**}} | **active** {**add hours** *start _time end _time* **days** *day* | **delete days** *day*} | **create** | **delete** | **match** {**device-type** {**add** | **delete**} *device-type* | **eap-type** {**add** | **delete**} {**eap-fast** | **eap-tls** | **leap** | **peap**} | **role** {*role_name* | **none**}}

構文の説明

policy_name	プロファイリング ポリシーの名前。
action	ポリシーのアクションを設定します。
acl	ポリシーの ACL を設定します。
enable	ポリシーのアクションを有効にします。
disable	ポリシーのアクションを無効にします。
acl_name	ACL の名前です。
average-data-rate	QoS 平均データ レートを設定します。
average-realtime-rate	QoS 平均リアルタイム レートを設定します。
burst-data-rate	QoS バースト データ レートを設定します。
burst-realtime-rate	QoS バーストリアルタイム レートを設定します。
qos	ポリシーの QoS アクションを設定します。
session-timeout	ポリシーのセッション タイムアウト アクションを設定します。
sleeping-client-timeout	ポリシーのスリープ クライアント タイムアウトを設定します。
avc-profile-name	ポリシーで AVC プロファイルを設定します。
vlan	ポリシーの VLAN アクションを設定します。
active	ポリシーのアクティブな時間および日を設定します。
add	アクティブな時間と日を追加します。
hours	ポリシーのアクティブな時間を設定します。

Start Time	ポリシーの開始時間。
End Time	ポリシーの終了時間。
days	ポリシーが機能する必要がある日を設定します。
day	曜日（**mon**、**tue**、**wed**、**thu**、**fri**、**sat**、**sun**など）。ポリシーが毎日または平日に機能するように daily または weekdays を指定することもできます。
delete	アクティブな時間と日を削除します。
create	ポリシーを作成します。
match	ポリシーの一致基準を設定します。
device-type	一致するデバイス タイプを設定します。
device-type	ポリシーを適用する必要があるデバイス タイプ。1 つのポリシーに最大 16 のデバイス タイプを設定できます。
eap-type	拡張可能認証プロトコル（EAP）タイプを一致基準として設定します。
eap-fast	EAP タイプを EAP セキュア トンネル経由フレキシブル認証（FAST）として設定します。
eap-tls	EAP タイプを EAP トランスポート層セキュリティ（TLS）として設定します。
leap	EAP タイプを Lightweight EAP（LEAP）として設定します。
peap	EAP タイプを Protected EAP（PEAP）として設定します。
role	ユーザのユーザ タイプまたはユーザ グループを設定します。
role_name	ユーザのユーザタイプまたはユーザグループ（学生、従業員など）。 ポリシーごとに 1 つのロールのみを設定できます。
none	ユーザのユーザ タイプまたはユーザ グループを設定しません。

コマンド デフォルト

Cisco WLC にはネイティブのプロファイリング ポリシーはありません。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

設定できるポリシーの最大数は 64 です。

次に、ポリシーのロールを設定する例を示します。

```
(Cisco Controller) > config policy student_policy role student
```

config port adminmode

特定のコントローラ ポートまたはすべてのポートの管理モードを有効または無効にするには、**config port adminmode** コマンドを使用します。

config port adminmode {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ポート 8 を無効にする例を示します。

```
(Cisco Controller) > config port adminmode 8 disable
```

次に、すべてのポートを有効にする例を示します。

```
(Cisco Controller) > config port adminmode all enable
```

config port autoneg

10/100BASE-Tイーサネット ポートで物理ポート自動ネゴシエーションを設定するには、**config port autoneg** コマンドを使用します。

config port autoneg {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

デフォルトでは、すべてのポートの自動ネゴシエーションが有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

config port physicalmode コマンドを使用して物理モードの手動設定を行う前に、ポート自動ネゴシエーションを無効にする必要があります。**config port autoneg** コマンドは、**config port physicalmode** コマンドを使用して行った設定を上書きします。

次に、前面パネルのすべてのイーサネット ポートで物理ポートの自動ネゴシエーションをオンにする例を示します。

```
(Cisco Controller) > config port autoneg all enable
```

次に、前面パネルのイーサネット ポート 19 で物理ポートの自動ネゴシエーションを無効にする例を示します。

```
(Cisco Controller) > config port autoneg 19 disable
```

config port linktrap

特定のコントローラ ポートまたはすべてのポートのリンク アップ/ダウン トラップを有効または無効にするには、**config port linktrap** コマンドを使用します。

config port linktrap {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

特定のコントローラ ポートまたはすべてのポートのダウンリンク トラップのデフォルト値は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ポート 8 のトラップを無効にする例を示します。

```
(Cisco Controller) > config port linktrap 8 disable
```

次に、すべてのポートのトラップを有効にする例を示します。

```
(Cisco Controller) > config port linktrap all enable
```

config port multicast appliance

特定のコントローラ ポートまたはすべてのポートのマルチキャスト アプライアンス サービスを有効または無効にするには、**config port multicast appliance** コマンドを使用します。

config port multicast appliance {**all** | *port*} {**enable** | **disable**}

構文の説明

all	すべてのポートを設定します。
port	ポート番号。
enable	指定したポートをイネーブルにします。
disable	指定したポートをディセーブルにします。

コマンド デフォルト

特定のコントローラ ポートまたはすべてのポートのデフォルトのマルチキャスト アプライアンス サービスは有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、すべてのポートでマルチキャスト アプライアンス サービスを有効にする例を示します。

```
(Cisco Controller) > config port multicast appliance all enable
```

次に、ポート 8 でマルチキャスト アプライアンス サービスを無効にする例を示します。

```
(Cisco Controller) > config port multicast appliance 8 disable
```

config prompt

CLI システム プロンプトを変更するには、**config prompt** コマンドを使用します。

config prompt *prompt*

構文の説明

prompt	二重引用符で囲まれた新しい CLI システム プロンプト。プロンプトには最大 31 文字の英数字を使用できます。また、大文字と小文字は区別されます。

コマンド デフォルト

システム プロンプトは起動ウィザードを使用して設定します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

システム プロンプトはユーザ定義変数であるため、このドキュメントの他の項では割愛します。

次に、Cisco 4400 への CLI システム プロンプトを変更する例を示します。

```
(Cisco Controller) > config prompt "Cisco 4400"
```

config qos average-data-rate

ユーザごとまたはサービス セット ID（SSID）ごとに TCP トラフィックの平均データ レートを Kbps 単位で定義するには、**config qos average-data-rate** コマンドを使用します。

config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

構文の説明

bronze	キューの平均データ レートを bronze に指定します。
silver	キューの平均データ レートを silver に指定します。
gold	キューの平均データ レートを gold に指定します。
platinum	キューの平均データ レートを platinum に指定します。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザ 1 人あたりの TCP トラフィックの平均データ レート。値は、0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、SSID ごとにキューの平均データ レート 0 Kbps を gold に設定する例を示します。

```
(Cisco Controller) > config qos average-data-rate gold per ssid downstream 0
```

関連コマンド

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos average-realtime-rate

ユーザごとまたはサービス セット ID（SSID）ごとに UDP トラフィックの平均リアルタイム データ レートを Kbps 単位で定義するには、**config qos average-realtime-rate** コマンドを使用します。

config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

構文の説明

bronze	キューの平均リアルタイム データ レートを bronze に指定します。
silver	キューの平均リアルタイム データ レートを silver に指定します。
gold	キューの平均リアルタイム データ レートを gold に指定します。
platinum	キューの平均リアルタイム データ レートを platinum に指定します。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザ 1 人あたりの UDP トラフィックの平均リアルタイム データ レート。値は、0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューの平均リアルタイムの実際のレートを gold に設定する例を示します。

```
(Cisco Controller) > config qos average-realtime-rate gold per ssid downstream 10
```

関連コマンド

config qos average-data-rate

config qos burst-data-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos burst-data-rate

ユーザごとまたはサービス セット ID（SSID）ごとに TCP トラフィックのピーク データ レートを Kbps 単位で定義するには、**config qos burst-data-rate** コマンドを使用します。

config qos burst-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

構文の説明

bronze	キューのピーク データ レートを bronze に指定します。
silver	キューのピーク データ レートを silver に指定します。
gold	キューのピーク データ レートを gold に指定します。
platinum	キューのピーク データ レートを platinum に指定します。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザ 1 人あたりの TCP トラフィックのピーク データ レート。値は、0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューのピーク レート 30000 kbps を gold に設定する例を示します。

```
(Cisco Controller) > config qos burst-data-rate gold per ssid downstream 30000
```

関連コマンド

config qos average-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config wlan override-rate-limit

config qos burst-realtime-rate

ユーザごとまたはサービス セット ID（SSID）ごとに UDP トラフィックのバースト リアルタイム データ レートを Kbps 単位で定義するには、**config qos burst-realtime-rate** コマンドを使用します。

config qos burst-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} { **per-ssid** | **per-client** } { **downstream** | **upstream** } *rate*

構文の説明

bronze	キューのバースト リアルタイム データ レートを bronze に指定します。
silver	キューのバースト リアルタイム データ レートを silver に指定します。
gold	キューのバースト リアルタイム データ レートを gold に指定します。
platinum	キューのバースト リアルタイム データ レートを platinum に指定します。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザ 1 人あたりの UDP トラフィックのバースト リアルタイム データ レート。値は、0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューのバースト リアルタイムの実際のレート 2000 kbps を gold に設定する例を示します。

```
(Cisco Controller) > config qos burst-realtime-rate gold per ssid downstream  2000
```

関連コマンド

config qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config wlan override-rate-limit

config qos description

プロファイルの説明を変更するには、**config qos description** コマンドを使用します。

config qos description {**bronze** | **silver** | **gold** | **platinum**} *description*

構文の説明

bronze	キューの QoS プロファイルの説明を bronze に指定します。
silver	キューの QoS プロファイルの説明を silver に指定します。
gold	キューの QoS プロファイルの説明を gold に指定します。
platinum	キューの QoS プロファイルの説明を platinum に指定します。
description	QoS プロファイルの説明。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューの QoS プロファイルの説明「description」を gold に設定する例を示します。

```
(Cisco Controller) > config qos description gold abc
```

関連コマンド

show qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config qos max-rf-usage

config qos max-rf-usage

アクセス ポイント 1 つあたりの RF 利用率の最大パーセンテージを設定するには、**config qos max-rf-usage** コマンドを使用します。

config qos max-rf-usage {**bronze** | **silver** | **gold** | **platinum**} *usage_percentage*

構文の説明

bronze	キューの RF 使用率の最大パーセントを bronze に指定します。
silver	キューの RF 使用率の最大パーセントを silver に指定します。
gold	キューの RF 使用率の最大パーセントを gold に指定します。
platinum	キューの RF 使用率の最大パーセントを platinum に指定します。
usage-percentage	RF 利用率の最大パーセンテージ。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キューの RF 使用率の最大パーセントを gold に指定する例を示します。

```
(Cisco Controller) > config qos max-rf-usage gold 20
```

関連コマンド

show qos description

config qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config qos burst-realtime-rate

config qos dot1p-tag

プロファイル内に分類されるパケットに関連付けられた優先タグの最大値（0 ～ 7）を定義するには、**config qos dot1p-tag** コマンドを使用します。

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *dot1p_tag*

構文の説明

bronze	キューの QoS 802.1p タグを bronze に設定します。
silver	キューの QoS 802.1p タグを silver に設定します。
gold	キューの QoS 802.1p タグを gold に設定します。
platinum	キューの QoS 802.1p タグを platinum に設定します。
dot1p_tag	1 ～ 7 の間の Dot1p タグの値。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、dot1p タグの値を 5 に設定して、キューの QoS 802.1p タグを gold に設定する例を示します。

```
(Cisco Controller) > config qos dot1p-tag gold 5
```

関連コマンド

show qos queue_length all

config qos protocol-type

config qos priority

QoSプロファイルをWLANに割り当てるときに、ユニキャストとマルチキャストのトラフィックに最大およびデフォルトの QoS レベルを定義するには、**config qos priority** コマンドを使用します。

config qos priority {**bronze** | **silver** | **gold** | **platinum**} {*maximum-priority* | *default-unicast-priority* | *default-multicast-priority*}

構文の説明

bronze	WLANのBronzeプロファイルを指定します。
silver	WLAN の Silver プロファイルを指定します。
gold	WLAN の Gold プロファイルを指定します。
platinum	WLAN の Platinum プロファイルを指定します。
maximum-priority	最大QoS優先度。次のいずれかを指定します。 • besteffort • background • video • voice
default-unicast-priority	デフォルト ユニキャストの優先度。次のいずれかを指定します。 • besteffort • background • video • voice
default-multicast-priority	デフォルト マルチキャストの優先度。次のいずれかを指定します。 • besteffort • background • video • voice

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

最大優先度レベルは、デフォルトのユニキャストとマルチキャストの優先度レベル以上にする必要があります。

次に、最大優先度として voice、デフォルト ユニキャスト優先度として video、およびデフォルト マルチキャスト優先度として besteffort を設定した WLAN の gold プロファイルに QoS 優先度を設定する例を示します。

```
(Cisco Controller) > config qos priority gold voice video besteffort
```

関連コマンド

config qos protocol-type

config qos protocol-type

プロファイル内に分類されるパケットに関連付けられた優先タグの最大値（0 ～ 7）を定義するには、**config qos protocol-type** コマンドを使用します。

config qos protocol-type {**bronze** | **silver** | **gold** | **platinum**} {**none** | *dot1p*}

構文の説明

bronze	キューの QoS 802.1p タグを bronze に設定します。
silver	キューの QoS 802.1p タグを silver に設定します。
gold	キューの QoS 802.1p タグを gold に設定します。
platinum	キューの QoS 802.1p タグを platinum に設定します。
none	特定のプロトコルが割り当てられていないときに指定します。
dot1p	dot1p タイプのプロトコルが割り当てられているときに指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、QoS プロトコル タイプを silver に設定する例を示します。

```
(Cisco Controller) > config qos protocol-type silver dot1p
```

関連コマンド

show qos queue_length all

config qos dot1p-tag

config qos queue_length

アクセス ポイントがキュー内に保持するパケットの最大数を指定するには、**config qos queue_length** コマンドを使用します。

config qos queue_length {**bronze** | **silver** | **gold** | **platinum**} *queue_length*

構文の説明

bronze	キューの QoS 長を bronze に指定します。
silver	キューの QoS 長を silver に指定します。
gold	キューの QoS 長を gold に指定します。
platinum	キューの QoS 長を platinum に指定します。
queue_length	キューの長さの最大値（10 ～ 255）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、最大キュー長の値を 12 に設定して、キューの QoS 長を「gold」に設定する例を示します。

```
(Cisco Controller) > config qos queue_length gold 12
```

関連コマンド

show qos

config qos qosmap

QoS マップを設定するには、**config qos qosmap** コマンドを使用します。

config qos qosmap {**enable** | **disable** | **default** }

構文の説明

enable	QoS マップ機能を有効にします。
disable	QoS マップ機能を無効にします。
default	デフォルトの QoS マップをリセットします。 QoS マップの値が 255（デフォルト）にリセットされます。また、DSCP UP 例外が存在しなければ追加します。DSCP UP 値をクリアするには、 **config qos qosmap clear-all** コマンドを入力します。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、QoS マップを有効にする例を示します。

```
(Cisco Controller) > config qos qosmap enable
```

config qos qosmap up-to-dscp-map

UP の DSCP 範囲を設定するには、**config qos qosmap** コマンドを使用します。

config qos qosmap up-to-dscp-map {*up dscp-default dscp-start dscp-end*}

構文の説明

up-to-dscp-map	UP の DSCP 範囲を設定します。
up	ワイヤレス UP 値。
dscp-default	この UP のデフォルト DSCP 値。
dscp-start	DSCP の開始範囲。範囲は 0 ~ 63 です。
dscp-end	DSCP の終了範囲。範囲は 0 ~ 63 です。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、UP の DSCP 範囲を設定する例を示します。

```
(Cisco Controller) > config qos qosmap up-to-dscp-map 2 3 5 20
```

config qos qosmap dscp-to-up-exception

DSCP 例外を設定するには、**config qos qosmap** コマンドを使用します。

config qos qosmap dscp-to-up-exception {*dscp up* }

構文の説明

dscp-to-up-exception	DSCP 例外の設定を許可します。
dscp	UP 値の例外 DSCP 値。
up	ワイヤレス ユーザ優先度（UP）値へのリンク。

次に、DSCP 例外を設定する例を示します。

```
(Cisco Controller) > config qos qosmap dscp-to-up-exception 3 1
```

config qos qosmap delete-dscp-exception

DSCP 例外を削除するには、**config qos qosmap** コマンドを使用します。

config qos qosmap delete-dscp-exception *dscp*

構文の説明

delete-dscp-exception	DSCP の例外を削除します。
dscp	UP の DSCP の例外

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、DSCP の例外を削除する例を示します。

```
(Cisco Controller) > config qos qosmap delete-dscp-exception 23
```

config qos qosmap clear-all

QoS マップからすべての例外を削除するには、**config qos qosmap** コマンドを使用します。

config qos qosmap clear-all

構文の説明		
	clear-all	すべての例外を削除します。

コマンド履歴		
	リリース	変更内容
	8.1	このコマンドが導入されました。

次に、QoS マップからすべての例外をクリアする例を示します。

```
(Cisco Controller) > config qos qosmap clear-all
```

config qos qosmap trust dscp upstream

クライアントの DSCP を使用してアップ ストリーム パケットをマーキングするには、**config qos qosmap** コマンドを使用します。

config qos qosmap trust-dscp-upstream {**enable** | **disable**}

構文の説明

trust-dscp-upstream	クライアントの DSCP に基づいてアップストリーム パケットがマーキングされます。
enable	クライアントの DSCP を使用したアップストリームパケットのマーキングを有効にします。
disable	クライアントの DSCP を使用したアップストリームパケットのマーキングを無効にします。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、クライアントの DSCP に基づいたパケット マーキングを有効にする例を示します。

```
(Cisco Controller) > config qos qosmap trust-dscp-upstream enable
```

config コマンド：r ～ z

- config radius acct （806 ページ）
- config radius acct ipsec authentication （810 ページ）
- config radius acct ipsec disable （811 ページ）
- config radius acct ipsec enable （812 ページ）
- config radius acct ipsec encryption （813 ページ）
- config radius acct ipsec ike （814 ページ）
- config radius acct mac-delimiter （815 ページ）
- config radius acct network （816 ページ）
- config radius acct realm （817 ページ）
- config radius acct retransmit-timeout （818 ページ）
- config radius auth （819 ページ）
- config radius auth callStationIdType （822 ページ）
- config radius auth framed-mtu （825 ページ）
- config radius auth IPsec authentication （826 ページ）
- config radius auth ipsec disable （827 ページ）
- config radius auth ipsec encryption （828 ページ）
- config radius auth ipsec ike （829 ページ）
- config radius auth keywrap （831 ページ）
- config radius auth mac-delimiter （832 ページ）
- config radius auth management （833 ページ）
- config radius auth mgmt-retransmit-timeout （834 ページ）
- config radius auth network （835 ページ）
- config radius auth realm （836 ページ）
- config radius auth retransmit-timeout （837 ページ）
- config radius auth rfc3576 （838 ページ）
- config radius auth retransmit-timeout （839 ページ）
- config radius aggressive-failover disabled （840 ページ）
- config radius backward compatibility （841 ページ）
- config radius callStationIdCase （842 ページ）

- config radius callStationIdType （843 ページ）
- config radius dns （846 ページ）
- config radius fallback-test （848 ページ）
- config radius ext-source-ports （850 ページ）
- config radius acct retransmit-timeout （851 ページ）
- config radius auth mgmt-retransmit-timeout （852 ページ）
- config radius auth retransmit-timeout （853 ページ）
- config radius auth retransmit-timeout （854 ページ）
- config redundancy interface address peer-service-port （855 ページ）
- config redundancy mobilitymac （856 ページ）
- config redundancy mode （857 ページ）
- config redundancy peer-route （858 ページ）
- config redundancy timer keep-alive-timer （859 ページ）
- config redundancy timer peer-search-timer （860 ページ）
- config redundancy unit （861 ページ）
- config remote-lan （862 ページ）
- config remote-lan aaa-override （863 ページ）
- config remote-lan acl （864 ページ）
- config remote-lan create （865 ページ）
- config remote-lan custom-web （866 ページ）
- config remote-lan delete （869 ページ）
- config remote-lan dhcp_server （870 ページ）
- config remote-lan exclusionlist （871 ページ）
- config remote-lan interface （872 ページ）
- config remote-lan ldap （873 ページ）
- config remote-lan mac-filtering （874 ページ）
- config remote-lan mab （875 ページ）
- config remote-lan max-associated-clients （876 ページ）
- config remote-lan radius_server （877 ページ）
- config remote-lan security （879 ページ）
- config remote-lan session-timeout （880 ページ）
- config remote-lan webauth-exclude （881 ページ）
- config rf-profile band-select （882 ページ）
- config rf-profile channel （884 ページ）
- config rf-profile client-trap-threshold （885 ページ）
- config rf-profile create （886 ページ）
- config rf-profile fra client-aware （887 ページ）
- config rf-profile data-rates （888 ページ）
- config rf-profile delete （890 ページ）
- config rf-profile description （891 ページ）
- config rf-profile load-balancing （892 ページ）

- config rf-profile max-clients （894 ページ）
- config rf-profile multicast data-rate （895 ページ）
- config rf-profile out-of-box （896 ページ）
- config rf-profile rx-sop threshold （897 ページ）
- config rf-profile trap-threshold （898 ページ）
- config rf-profile tx-power-control-thresh-v1 （899 ページ）
- config rf-profile tx-power-control-thresh-v2 （900 ページ）
- config rf-profile tx-power-max （901 ページ）
- config rf-profile tx-power-min （902 ページ）
- config rogue ap timeout （903 ページ）
- config rogue adhoc （904 ページ）
- config rogue ap classify （908 ページ）
- config rogue ap friendly （910 ページ）
- config rogue ap rldp （912 ページ）
- config rogue ap ssid （914 ページ）
- config rogue ap timeout （916 ページ）
- config rogue auto-contain level （917 ページ）
- config rogue ap valid-client （919 ページ）
- config rogue client （921 ページ）
- config rogue containment （923 ページ）
- config rogue detection （924 ページ）
- config rogue detection client-threshold （925 ページ）
- config rogue detection min-rssi （926 ページ）
- config rogue detection monitor-ap （927 ページ）
- config rogue detection report-interval （929 ページ）
- config rogue detection security-level （930 ページ）
- config rogue detection transient-rogue-interval （931 ページ）
- config rogue rule （932 ページ）
- config rogue rule condition ap （937 ページ）
- config remote-lan session-timeout （939 ページ）
- config rfid auto-timeout （940 ページ）
- config rfid status （941 ページ）
- config rfid timeout （942 ページ）
- config rogue ap timeout （943 ページ）
- config route add （944 ページ）
- config route delete （945 ページ）
- config serial baudrate （946 ページ）
- config serial timeout （947 ページ）
- config service timestamps （948 ページ）
- config sessions maxsessions （949 ページ）
- config sessions timeout （950 ページ）

- config slot （951 ページ）
- config switchconfig boot-break （953 ページ）
- config switchconfig fips-prerequisite （954 ページ）
- config switchconfig ucapl （955 ページ）
- config switchconfig wlancc （956 ページ）
- config switchconfig strong-pwd （957 ページ）
- config switchconfig flowcontrol （960 ページ）
- config switchconfig mode （961 ページ）
- config switchconfig secret-obfuscation （962 ページ）
- config sysname （963 ページ）
- config snmp community accessmode （964 ページ）
- config snmp community create （965 ページ）
- config snmp community delete （966 ページ）
- config snmp community ipaddr （967 ページ）
- config snmp community mode （968 ページ）
- config snmp engineID （969 ページ）
- config snmp syscontact （970 ページ）
- config snmp syslocation （971 ページ）
- config snmp trapreceiver create （972 ページ）
- config snmp trapreceiver delete （973 ページ）
- config snmp trapreceiver mode （974 ページ）
- config snmp v3user create （975 ページ）
- config snmp v3user delete （977 ページ）
- config snmp version （978 ページ）
- config tacacs acct （979 ページ）
- config tacacs athr （981 ページ）
- config tacacs athr mgmt-server-timeout （983 ページ）
- config tacacs auth （984 ページ）
- config tacacs auth mgmt-server-timeout （986 ページ）
- config tacacs dns （987 ページ）
- config tacacs fallback-test interval （989 ページ）
- config time manual （990 ページ）
- config time ntp （991 ページ）
- config time timezone （994 ページ）
- config time timezone location （995 ページ）
- config trapflags 802.11-Security （999 ページ）
- config trapflags aaa （1000 ページ）
- config trapflags adjchannel-rogueap （1001 ページ）
- config trapflags ap （1002 ページ）
- config trapflags authentication （1003 ページ）
- config trapflags client （1004 ページ）

- config trapflags client max-warning-threshold （1006 ページ）
- config trapflags configsave （1007 ページ）
- config trapflags IPsec （1008 ページ）
- config trapflags linkmode （1010 ページ）
- config trapflags mesh （1011 ページ）
- config trapflags multiusers （1012 ページ）
- config trapflags rfid （1013 ページ）
- config trapflags rogueap （1015 ページ）
- config trapflags rrm-params （1016 ページ）
- config trapflags rrm-profile （1017 ページ）
- config trapflags stpmode （1018 ページ）
- config trapflags strong-pwdcheck （1019 ページ）
- config trapflags wps （1020 ページ）
- config tunnel eogre heart-beat （1021 ページ）
- config tunnel eogre gateway （1022 ページ）
- config tunnel eogre domain （1023 ページ）
- config tunnel profile （1024 ページ）
- config tunnel profile_rule （1025 ページ）
- config tunnel profile_rule-delete （1026 ページ）
- config tunnel profile eogre-DHCP82 （1027 ページ）
- config tunnel profile eogre-gateway-radius-proxy （1028 ページ）
- config tunnel profile eogre-gateway-radius-proxy-accounting （1029 ページ）
- config tunnel profile eogre-DHCP82 （1030 ページ）
- config tunnel profile eogre-DHCP82-circuit-id （1031 ページ）
- config tunnel profile eogre-DHCP82-delimiter （1032 ページ）
- config tunnel profile eogre-DHCP82-format （1033 ページ）
- config tunnel profile eogre-DHCP82-remote-id （1034 ページ）
- config watchlist add （1035 ページ）
- config watchlist delete （1036 ページ）
- config watchlist disable （1037 ページ）
- config watchlist enable （1038 ページ）
- config wgb vlan （1039 ページ）
- config wlan （1040 ページ）
- config wlan 7920-support （1042 ページ）
- config wlan 802.11e （1043 ページ）
- config wlan aaa-override （1044 ページ）
- config wlan acl （1046 ページ）
- config wlan apgroup （1047 ページ）
- config wlan apgroup atf 802.11 （1056 ページ）
- config wlan apgroup atf 802.11 policy （1057 ページ）
- config wlan apgroup qinq （1058 ページ）

- config wlan assisted-roaming （1060 ページ）
- config wlan atf （1061 ページ）
- config wlan avc （1062 ページ）
- config wlan band-select allow （1063 ページ）
- config wlan broadcast-ssid （1064 ページ）
- config wlan call-snoop （1065 ページ）
- config wlan chd （1066 ページ）
- config wlan ccx aironet-ie （1067 ページ）
- config wlan channel-scan defer-priority （1068 ページ）
- config wlan channel-scan defer-time （1069 ページ）
- config wlan custom-web （1070 ページ）
- config wlan dhcp_server （1072 ページ）
- config wlan diag-channel （1073 ページ）
- config wlan dtim （1074 ページ）
- config wlan exclusionlist （1075 ページ）
- config wlan fabric （1076 ページ）
- config wlan flexconnect ap-auth （1077 ページ）
- config wlan flexconnect central-assoc （1078 ページ）
- config wlan flexconnect learn-ipaddr （1079 ページ）
- config wlan flexconnect local-switching （1080 ページ）
- config wlan flexconnect vlan-central-switching （1082 ページ）
- config wlan flow （1083 ページ）
- config wlan hotspot （1084 ページ）
- config wlan hotspot dot11u （1085 ページ）
- config wlan hotspot dot11u 3gpp-info （1086 ページ）
- config wlan hotspot dot11u auth-type （1087 ページ）
- config wlan hotspot dot11u disable （1088 ページ）
- config wlan hotspot dot11u domain （1089 ページ）
- config wlan hotspot dot11u enable （1090 ページ）
- config wlan hotspot dot11u hessid （1091 ページ）
- config wlan hotspot dot11u ipaddr-type （1092 ページ）
- config wlan hotspot dot11u nai-realm （1093 ページ）
- config wlan hotspot dot11u network-type （1096 ページ）
- config wlan hotspot dot11u roam-oi （1097 ページ）
- config wlan hotspot hs2 （1098 ページ）
- config wlan hotspot hs2 domain-id （1101 ページ）
- config wlan hotspot hs2 osu legacy-ssid （1102 ページ）
- config wlan hotspot hs2 osu sp create （1103 ページ）
- config wlan hotspot hs2 osu sp delete （1104 ページ）
- config wlan hotspot hs2 osu sp icon-file add （1105 ページ）
- config wlan hotspot hs2 osu sp icon-file delete （1106 ページ）

- config wlan hotspot hs2 osu sp method add （1107 ページ）
- config wlan hotspot hs2 osu sp method delete （1108 ページ）
- config wlan hotspot hs2 osu sp nai add （1109 ページ）
- config wlan hotspot hs2 osu sp nai delete （1110 ページ）
- config wlan hotspot hs2 osu sp uri add （1111 ページ）
- config wlan hotspot hs2 osu sp uri delete （1112 ページ）
- config wlan hotspot hs2 wan-metrics downlink （1113 ページ）
- config wlan hotspot hs2 wan-metrics link-status （1114 ページ）
- config wlan hotspot hs2 wan-metrics lmd （1115 ページ）
- config wlan hotspot hs2 wan-metrics uplink （1116 ページ）
- config wlan hotspot msap （1117 ページ）
- config wlan interface （1118 ページ）
- config wlan ipv6 acl （1119 ページ）
- config wlan kts-cac （1120 ページ）
- config wlan layer2 acl （1121 ページ）
- config wlan ldap （1122 ページ）
- config wlan learn-ipaddr-cswlan （1123 ページ）
- config wlan load-balance （1124 ページ）
- config wlan mac-filtering （1125 ページ）
- config wlan max-associated-clients （1126 ページ）
- config wlan max-radio-clients （1127 ページ）
- config wlan mdns （1128 ページ）
- config wlan media-stream （1129 ページ）
- config wlan mfp （1130 ページ）
- config wlan mobility anchor （1131 ページ）
- config wlan mobility foreign-map （1132 ページ）
- config wlan multicast buffer （1133 ページ）
- config wlan multicast interface （1134 ページ）
- config wlan mu-mimo （1135 ページ）
- config wlan nac （1136 ページ）
- config wlan override-rate-limit （1137 ページ）
- config wlan passive-client （1139 ページ）
- config wlan peer-blocking （1140 ページ）
- config wlan pmipv6 default-realm （1141 ページ）
- config wlan pmipv6 mobility-type （1142 ページ）
- config wlan pmipv6 profile_name （1143 ページ）
- config wlan policy （1144 ページ）
- config wlan profile （1145 ページ）
- config wlan profiling （1146 ページ）
- config wlan qos （1148 ページ）
- config wlan radio （1149 ページ）

- config wlan radius_server acct （1150 ページ）
- config wlan radius_server acct interim-update （1152 ページ）
- config wlan radius_server auth （1153 ページ）
- config wlan radius_server overwrite-interface （1154 ページ）
- config wlan radius_server realm （1155 ページ）
- config wlan roamed-voice-client re-anchor （1156 ページ）
- config wlan security 802.1X （1157 ページ）
- config wlan security ckip （1159 ページ）
- config wlan security cond-web-redir （1161 ページ）
- config wlan security eap-params （1162 ページ）
- config wlan security eap-passthru （1164 ページ）
- config wlan security ft （1165 ページ）
- config wlan security ft over-the-ds （1166 ページ）
- config wlan security IPsec disable （1167 ページ）
- config wlan security IPsec enable （1168 ページ）
- config wlan security IPsec authentication （1169 ページ）
- config wlan security IPsec encryption （1170 ページ）
- config wlan security IPsec config （1171 ページ）
- config wlan security IPsec ike authentication （1172 ページ）
- config wlan security IPsec ike dh-group （1173 ページ）
- config wlan security IPsec ike lifetime （1174 ページ）
- config wlan security IPsec ike phase1 （1175 ページ）
- config wlan security IPsec ike contivity （1176 ページ）
- config wlan security wpa akm ft （1177 ページ）
- config wlan security ft （1178 ページ）
- config wlan security passthru （1179 ページ）
- config wlan security pmf （1180 ページ）
- config wlan security splash-page-web-redir （1182 ページ）
- config wlan security static-wep-key authentication （1183 ページ）
- config wlan security static-wep-key disable （1184 ページ）
- config wlan security static-wep-key enable （1185 ページ）
- config wlan security static-wep-key encryption （1186 ページ）
- config wlan security tkip （1187 ページ）
- config wlan usertimeout （1188 ページ）
- config wlan security web-auth （1189 ページ）
- config wlan security web-passthrough acl （1191 ページ）
- config wlan security web-passthrough disable （1192 ページ）
- config wlan security web-passthrough email-input （1193 ページ）
- config wlan security web-passthrough enable （1194 ページ）
- config wlan security wpa akm 802.1x （1195 ページ）
- config wlan security wpa akm cckm （1196 ページ）

- config wlan security wpa akm ft （1197 ページ）
- config wlan security wpa akm pmf （1198 ページ）
- config wlan security wpa akm psk （1199 ページ）
- config wlan security wpa disable （1200 ページ）
- config wlan security wpa enable （1201 ページ）
- config wlan security wpa ciphers （1202 ページ）
- config wlan security wpa gtk-random （1203 ページ）
- config wlan security wpa osen disable （1204 ページ）
- config wlan security wpa osen enable （1205 ページ）
- config wlan security wpa wpa1 disable （1206 ページ）
- config wlan security wpa wpa1 enable （1207 ページ）
- config wlan security wpa wpa2 disable （1208 ページ）
- config wlan security wpa wpa2 enable （1209 ページ）
- config wlan security wpa wpa2 cache （1210 ページ）
- config wlan security wpa wpa2 cache sticky （1211 ページ）
- config wlan security wpa wpa2 ciphers （1212 ページ）
- config wlan session-timeout （1213 ページ）
- config wlan sip-cac disassoc-client （1215 ページ）
- config wlan sip-cac send-486busy （1216 ページ）
- config wlan ssid （1217 ページ）
- config wlan static-ip tunneling （1218 ページ）
- config wlan uapsd compliant client enable （1219 ページ）
- config wlan uapsd compliant-client disable （1220 ページ）
- config wlan user-idle-threshold （1221 ページ）
- config wlan usertimeout （1222 ページ）
- config wlan webauth-exclude （1223 ページ）
- config wlan wifidirect （1224 ページ）
- config wlan wmm （1225 ページ）
- config wps ap-authentication （1226 ページ）
- config wps auto-immune （1227 ページ）
- config wps cids-sensor （1228 ページ）
- config wps client-exclusion （1230 ページ）
- config wps mfp （1232 ページ）
- config wps shun-list re-sync （1233 ページ）
- config wps signature （1234 ページ）
- config wps signature frequency （1236 ページ）
- config wps signature interval （1237 ページ）
- config wps signature mac-frequency （1238 ページ）
- config wps signature quiet-time （1239 ページ）
- config wps signature reset （1240 ページ）

config radius acct

Cisco ワイヤレス LAN コントローラ の RADIUS アカウンティング サーバの設定を行うには、**config radius acct** コマンドを使用します。

config radius acct{ {**add** *index IP addr port* {**ascii** | **hex**} *secret*} | **delete** *index* | **disable** *index* | **enable** *index* | **ipsec** {**authentication** {**hmac-md5** *index* | **hmac-sha1** *index* } | **disable** *index* | **enable** *index* | **encryption** {**256-aes** | **3des** | **aes** | **des**} *index* | **ike** {**auth-mode** {**pre-shared-key** *index type shared_secret_key* | **certificate** *index* } | **dh-group** { **2048bit-group-14** | **group-1** | **group-2** | **group-5**} *index* | **lifetime** *seconds index* | **phase1** {**aggressive** | **main**} *index* } } | {**mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**}} | {**network** *index* {**disable** | **enable**}} | {**region** {**group** | **none** | **provincial**}} | **retransmit-timeout** *index seconds* | **realm** {**add** | **delete**} *index realm-string*}

構文の説明

add	RADIUS アカウンティング サーバ（IPv4 または IPv6）を追加します。
index	RADIUS サーバ インデックス（1 ～ 17）。
ip-addr	RADIUS サーバの IP アドレス（IPv4 または IPv6）。
port	RADIUS サーバのインターフェイス プロトコルの UDP ポート番号。
ascii	RADIUS サーバの共有キーのタイプ（**ascii**）を指定します。
hex	RADIUS サーバの共有キーのタイプ（**hex**）を指定します。
secret	RADIUS サーバのシークレット。
enable	RADIUS アカウンティング サーバを有効にします。
disable	RADIUS アカウンティング サーバを無効にします。
delete	RADIUS アカウンティング サーバを削除します。
ipsec	アカウンティング サーバに対する IPSec サポートを有効または無効にします。 （注） IPSec は IPv6 ではサポートされません。

authentication	IPSec 認証を設定します。
hmac-md5	IPSec HMAC-MD5 認証を有効にします。
hmac-sha1	IPSec HMAC-SHA1 認証を有効にします。
disable	アカウンティング サーバに対する IPSec サポートを無効にします。
enable	アカウンティング サーバに対する IPSec サポートを有効にします。
encryption	IPSec 暗号化を設定します。
256-aes	IPSec AES 暗号化を有効にします。
3des	IPSec 3DES 暗号化を有効にします。
aes	IPSec AES-128 暗号化を有効にします。
des	IPSec DES 暗号化を有効にします。
ike	インターネット キー エクスチェンジ（IKE）を設定します。
auth-mode	IKE 認証方式を設定します。
pre-shared-key	認証の事前共有キー。
certificate	認証に使用される証明書。
dh-group	IKE Diffie-Hellman グループを設定します。
2048bit-group-14	DH グループ 14（2048 ビット）を設定します。
group-1	DH グループ 1（768 ビット）を設定します。
group-2	DH グループ 2（1024 ビット）を設定します。
group-5	DH グループ 5（1536 ビット）を設定します。
lifetime *seconds*	IKE ライフタイム（秒単位）を設定します。指定できる範囲は 1800 ～ 57600 秒です。デフォルトは 28800 秒です。
phase1	IKE phase1 モードを設定します。
aggressive	IKE アグレッシブ モードを有効にします。
main	IKE メイン モードを有効にします。

mac-delimiter	コール元ステーション ID とコール先ステーション ID の MAC デリミタを設定します。
colon	デリミタをコロンに設定します（xx:xx:xx:xx:xx:xx など）。
hyphen	デリミタをハイフンに設定します（xx-xx-xx-xx-xx-xx など）。
none	デリミタを無効にします（xxxxxxxxxx など）。
single-hyphen	デリミタを単一ハイフンに設定します（xxxxxx-xxxxxx など）。
network	ネットワーク ユーザのデフォルト RADIUS サーバを設定します。
group	RADIUS サーバ タイプを group に指定します。
none	RADIUS サーバ タイプを none に指定します。
provincial	RADIUS サーバ タイプを provincial に指定します。
retransmit-timeout	サーバのデフォルト再送信タイムアウトを変更します。
seconds	再送信の間隔（秒単位）。
realm	RADIUS アカウンティング レルムを指定します。
add	RADIUS アカウンティング レルムを追加します。
delete	RADIUS アカウンティング レルムを削除します。

コマンド デフォルト

RADIUS サーバの追加時、ポート番号は 1813 にデフォルト設定され、状態が **enabled** になります。

使用上のガイドライン

IPSec は IPv6 ではサポートされません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

リリース	変更内容
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、ポート *1813* で *admin* のログイン パスワードを使用して、*10.10.10.10* にある優先順位 1 の RADIUS アカウンティング サーバを設定する例を示します。

```
(Cisco Controller) > config radius acct add 1 10.10.10.10 1813 ascii admin
```

次に、ポート *1813* で *admin* のログイン パスワードを使用して、*2001:9:6:40::623* にある優先順位 1 の RADIUS アカウンティング サーバを設定する例を示します。

```
(Cisco Controller) > config radius acct add 1 2001:9:6:40::623 1813 ascii admin
```

config radius acct ipsec authentication

Cisco ワイヤレス LAN コントローラで IPSec 認証を設定するには、**config radius acct ipsec authentication** コマンド使用します。

config radius acct ipsec authentication {**hmac-md5** | **hmac-sha1**} *index*

構文の説明

hmac-md5	IPsec HMAC-MD5 認証をイネーブルにします。
hmac-sha1	IPsec HMAC-SHA1 認証をイネーブルにします。
index	RADIUS サーバ インデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS アカウンティング サーバ インデックス 1 で IPSec hmac-md5 認証サービスを設定する例を示します。

```
(Cisco Controller) > config radius acct ipsec authentication hmac-md5 1
```

関連コマンド

show radius acct statistics

config radius acct ipsec disable

Cisco ワイヤレス LAN コントローラのアカウンティング サーバに対する IPSec サポートを無効にするには、**config radius acct ipsec disable** コマンドを使用します。

config radius acct ipsec disable *index*

構文の説明

index	RADIUS サーバ インデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS アカウンティング サーバ インデックス 1 に対する IPSec サポートを無効にする例を示します。

```
(Cisco Controller) > config radius acct ipsec disable 1
```

関連コマンド

show radius acct statistics

config radius acct ipsec enable

Cisco ワイヤレス LAN コントローラのアカウンティング サーバに対する IPSec サポートを有効にするには、**config radius acct ipsec enable** コマンドを使用します。

config radius acct ipsec enable *index*

構文の説明

index	RADIUS サーバ インデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

例

次に、RADIUS アカウンティング サーバ インデックス 1 に対する IPSec サポートを有効にする例を示します。

```
(Cisco Controller) > config radius acct ipsec enable 1
```

関連コマンド

show radius acct statistics

config radius acct ipsec encryption

Cisco ワイヤレス LAN コントローラのアカウンティング サーバに IPSec 暗号化を設定するには、**config radius acct ipsec encryption** コマンドを使用します。

config radius acct ipsec encryption {**3des** | **aes** | **des**} *index*

構文の説明

256-aes	IPSec AES-256 暗号化を有効にします。
3des	IPSec 3DES 暗号化をイネーブルにします。
aes	IPSec AES 暗号化を有効にします。
des	IPSec DES 暗号化をイネーブルにします。
index	RADIUS サーバのインデックス値（1 ～ 17）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS サーバのインデックス値 3 の IPSec 3DES 暗号化を設定する例を示します。

```
(Cisco Controller) > config radius acct ipsec encryption 3des 3
```

config radius acct ipsec ike

Cisco WLC でインターネット キー交換（IKE）を設定するには、**config radius acct ipsec ike** コマンドを使用します。

config radius acct ipsec ike dh-group {**group-1** | **group-2** | **group-5** | **group-14**} | **lifetime** *seconds* | **phase1** {**aggressive** | **main**}} *index*

構文の説明

dh-group	Dixie-Hellman（DH）グループを指定します。
group-1	DH グループ 1（768 ビット）を設定します。
group-2	DH グループ 2（1024 ビット）を設定します。
group-5	DH グループ 5（1024 ビット）を設定します。
group-5	DH グループ 14（2048 ビット）を設定します。
lifetime	IKE ライフタイムを設定します。
seconds	IKE の有効期間（秒単位）。
phase1	IKE phase1 ノードを設定します。
aggressive	アグレッシブ モードをイネーブルにします。
main	メイン モードをイネーブルにします。
index	RADIUS サーバ インデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS サーバ インデックス 1 の IKE の有効期間を 23 秒に設定する例を示します。

```
(Cisco Controller) > config radius acct ipsec ike lifetime 23 1
```

関連コマンド

show radius acct statistics

config radius acct mac-delimiter

RADIUS アカウンティング サーバに送信される MAC アドレスで使用されるデリミタを指定するには、**config radius acct mac-delimiter** コマンドを使用します。

config radius acct mac-delimiter {**colon** | **hyphen** | **single-hyphen** | **none**}

構文の説明

colon	デリミタをコロンに設定します（xx:xx:xx:xx:xx:xx など）。
hyphen	デリミタをハイフンに設定します（xx-xx-xx-xx-xx-xx など）。
single-hyphen	デリミタを単一ハイフンに設定します（xxxxxx-xxxxxx など）。
none	デリミタを無効にします（xxxxxxxxxxxx など）。

コマンド デフォルト

デフォルトのデリミタは、ハイフンです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ネットワーク ユーザの RADIUS アカウンティング サーバに送信される MAC アドレスで使用されるデリミタ ハイフンを設定する例を示します。

```
(Cisco Controller) > config radius acct mac-delimiter hyphen
```

関連コマンド

show radius acct statistics

config radius acct network

ネットワーク ユーザのデフォルト RADIUS サーバを設定するには、**config radius acct network** コマンドを使用します。

config radius acct network *index* {**enable** | **disable**}

構文の説明

index	RADIUS サーバ インデックス。
enable	サーバをネットワーク ユーザのデフォルト RADIUS サーバとして有効にします。
disable	サーバをネットワーク ユーザのデフォルト RADIUS サーバとして無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS サーバ インデックス 1 でネットワーク ユーザのデフォルト RADIUS アカウンティング サーバを設定する例を示します。

```
(Cisco Controller) > config radius acct network 1 enable
```

関連コマンド

show radius acct statistics

config radius acct realm

RADIUS アカウンティング サーバでレルムを設定するには、**config radius acct realm** コマンドを使用します。

config radius acct realm {**add** | **delete**} *radius_index realm_string*

構文の説明

radius_server	RADIUS サーバ インデックス。範囲は 1 ～ 17 です。
add	RADIUS アカウンティング サーバにレルムを追加します。
delete	RADIUS アカウンティング サーバからレルムを削除します。
realm_string	RADIUS アカウンティング レルムに関連付けられた一意の文字列です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、RADIUS アカウンティング サーバにレルムを追加する例を示します。

```
(Cisco Controller) > config radius acct realm add 3 test
```

config radius acct retransmit-timeout

Cisco ワイヤレス LAN コントローラ の RADIUS アカウンティング サーバのデフォルト送信タイムアウトを変更するには、**config radius acct retransmit-timeout** コマンドを使用します。

config radius acct retransmit-timeout *index timeout*

構文の説明

index	RADIUS サーバ インデックス。
timeout	秒単位での再送信間隔（2 ～ 30）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、再送信間隔の再送信タイムアウト値を 5 秒に設定する例を示します。

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

関連コマンド

show radius acct statistics

config radius auth

Cisco ワイヤレス LAN コントローラ の RADIUS 認証サーバの設定を行うには、**config radius auth** コマンドを使用します。

config radius auth {**add** *index IP addr portascii/hexsecret*} | | **delete** *index* | **disable** *index* | **enable** *index* | **framed-mtu** *mtu* | { **ipsec** {**authentication** {**hmac-md5** *index* | **hmac-sha1** *index* } | **disable** *index* | **enable** *index* | **encryption** {**256-aes** | **3des** | **aes** | **des**} *index* | **ike** {**auth-mode** {**pre-shared-key** *index ascii/hex shared_secret* | **certificate** *index* } | **dh-group** { **2048bit-group-14** | **group-1** | **group-2** | **group-5**} *index* | **lifetime** *seconds index* | **phase1** {**aggressive** | **main**} *index* } } | { { **keywrap**{**add** *ascii/hex kek mack index* } | **delete** *index* | **disable** | **enable**} } | {**mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**}} | {{**management** *index* {**enable** | **disable**}} | { **mgmt-retransmit-timeout** *index Retransmit Timeout* } | { **network** *index* {**enable** | **disable**}} | {**realm** {**add** | **delete**} *radius-index realm-string*} } | {**region** {**group** | **none** | **provincial**}} | {**retransmit-timeout** *index Retransmit Timeout*} | { **rfc3576** {**enable** | **disable**} *index* }

構文の説明

enable	RADIUS 認証サーバを有効にします。
disable	RADIUS 認証サーバを無効にします。
delete	RADIUS 認証サーバを削除します。
index	RADIUS サーバ インデックス。コントローラは、1 で検索を開始します。サーバ インデックスの範囲は 1 ～ 17 です。
add	RADIUS 認証サーバを追加します。「デフォルト」の項を参照してください。
ip-addr	RADIUS サーバの IP アドレス（IPv4 または IPv6）です。
port	RADIUS サーバのインターフェイス プロトコルの UDP ポート番号。
ascii/hex	RADIUS サーバの秘密キーのタイプ（**ascii** または **hex**）を指定します。
secret	RADIUS サーバのシークレット。
callStationIdType	RADIUS 認証メッセージで送信されるコール先ステーション ID 情報を設定します。
framed-mtu	すべての RADIUS サーバの Framed-MTU を設定します。Framed-MTU の範囲は 64 ～ 1300 バイトです。

ipsec	認証サーバの IPSec サポートを有効または無効にします。 （注） IPSec は IPv6 ではサポートされません。
keywrap	RADIUS キーラップを設定します。
ascii/hex	キーラップ キーの入力形式を指定します。
kek	16 バイトのキー暗号化キーを入力します。
mack	20 バイトのメッセージ オーセンティケータ コード キーを入力します。
mac-delimiter	コール元ステーション ID とコール先ステーション ID の MAC デリミタを設定します。
management	管理ユーザの RADIUS サーバを設定します。
mgmt-retransmit-timeout	サーバのデフォルト管理ログイン再送信タイムアウトを変更します。
network	ネットワーク ユーザのデフォルト RADIUS サーバを設定します。
realm	RADIUS 認証レルムを設定します。
region	RADIUS リージョンプロパティを設定します。
retransmit-timeout	サーバのデフォルト ネットワーク ログイン再送信タイムアウトを変更します。
rfc3576	認証サーバに対する RFC-3576 サポートを有効または無効にします。

コマンド デフォルト

RADIUS サーバの追加時、ポート番号は 1812 にデフォルト設定され、状態が **enabled** になります。

使用上のガイドライン

IPSec は IPv6 ではサポートされません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、ポート *1812* で *admin* のログイン パスワードを使用して、*10.10.10.10* にある優先順位 *3* の RADIUS 認証サーバを設定する例を示します。

```
(Cisco Controller) > config radius auth add 3 10.10.10.10 1812 ascii admin
```

次に、ポート *1812* で *admin* のログイン パスワードを使用して、 *2001:9:6:40::623* にある優先順位 *3* の RADIUS 認証サーバを設定する例を示します。

```
(Cisco Controller) > config radius auth add 3 2001:9:6:40::623 1812 ascii admin
```

config radius auth callStationIdType

RADIUS 認証サーバを設定するには、**config radius auth callStationIdType** コマンドを使用します。

config radius auth callStationIdType {**ap-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddr-only** | **ap-macaddr-ssid** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **ipaddr** | **macaddr** | **vlan-id**}

構文の説明

ipaddr	IP アドレスを使用する呼出端末 ID タイプを設定します（レイヤ 3 のみ）。
macaddr	システムの MAC アドレスを使用する呼出端末 ID タイプを設定します（レイヤ 2 およびレイヤ 3）。
ap-macaddr-only	アクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定します（レイヤ 2 およびレイヤ 3）。
ap-macaddr-ssid	*AP MAC address*:*SSID* の形式でアクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定します（レイヤ 2 およびレイヤ 3）。
ap-ethmac-only	アクセス ポイントのイーサネット MAC アドレスを使用する着信端末 ID タイプを設定します。
ap-ethmac-ssid	*AP Ethernet MAC address*:*SSID* の形式でアクセス ポイントのイーサネット MAC アドレスを使用する着信端末 ID タイプを設定します。
ap-group-name	AP グループ名を使用する呼出端末 ID タイプを設定します。AP が AP グループの一部でない場合、「default-group」が AP グループ名として使用されます。
flex-group-name	FlexConnect グループ名を使用する呼出端末 ID タイプを設定します。FlexConnect AP が FlexConnect グループの一部でない場合、システム MAC アドレスが呼出端末 ID として使用されます。
ap-name	アクセス ポイントの名前を使用する呼出端末 ID タイプを設定します。

ap-name-ssid	*AP name*:*SSID* の形式でアクセス ポイントの名前を使用する呼出端末 ID タイプを設定します。
ap-location	アクセス ポイントのロケーションを使用する呼出端末 ID タイプを設定します。
vlan-id	システムの VLAN-ID を使用する呼出端末 ID タイプを設定します。
ap-label-address	呼出端末ID タイプを、アカウンティング メッセージの AP ラベルに印刷されている AP MAC アドレスに設定します。
ap-label-address-ssid	呼出端末 ID タイプを、AP MAC address:SSID 形式に設定します。

コマンド デフォルト

システムの MAC アドレス。

使用上のガイドライン

コントローラは、すべての認証パケットおよびアカウンティング パケットで RADIUS サーバに着信端末 ID 属性を送信します。着信端末 ID 属性を使用すると、属性値に基づいて、異なるグループにユーザを分類できます。コマンドは着信端末に対してのみ適用可能であり、発信端末には適用できません。

SSID のみを Calling-Station-ID として送信することはできません。SSID は、アクセス ポイント MAC アドレスまたはアクセス ポイント名のいずれかにのみ組み合わせることができます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
7.6	アクセス ポイントのイーサネット MAC アドレスをサポートするために **ap-ethmac-only** キーワードと **ap-ethmac-ssid** キーワードが追加されました。 **ap-label-address** および **ap-label-address-ssid** キーワードが追加されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、IP アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius auth callStationIdType ipAddr
```

次に、システムの MAC アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius auth callStationIdType macAddr
```

次に、アクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius auth callStationIdType ap-macAddr
```

config radius auth framed-mtu

すべての RADIUS サーバの Framed-MTU 値を設定するには、**config radius auth framed-mtu** コマンドを使用します。

config radius auth framed-mtu *mtu*

構文の説明

mtu	Framed-MTU 値の範囲は 64 ー 1300 バイトです。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。

次に、RADIUS 認証サーバの Framed-MTU 値を設定する例を示します。

```
(Cisco Controller) > config radius auth framed-mtu 500
```

config radius auth IPsec authentication

Cisco ワイヤレス LAN コントローラの認証サーバに対する IPSec サポートを設定するには、**config radius auth IPsec authentication** コマンドを使用します。

config radius auth IPsec authentication {**hmac-md5** | **hmac-sha1**} *index*

構文の説明

hmac-md5	IPsec HMAC-MD5 認証をイネーブルにします。
hmac-shal	IPsec HMAC-SHA1 認証をイネーブルにします。
index	RADIUS サーバ インデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバ インデックス 1 に対する IPSec hmac-md5 サポートを設定する例を示します。

```
(Cisco Controller) > config radius auth IPsec authentication hmac-md5 1
```

関連コマンド

show radius acct statistics

config radius auth ipsec disable

Cisco ワイヤレス LAN コントローラの認証サーバに対する IPSec サポートを無効するには、**config radius auth IPsec disable** コマンドを使用します。

config radius auth ipsec {**enable** | **disable**} *index*

構文の説明

enable	認証サーバの IPSec サポートを有効にします。
disable	認証サーバの IPSec サポートを無効にします。
index	RADIUS サーバ インデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバ インデックス 1 に対する IPSec サポートを有効にする例を示します。

```
(Cisco Controller) > config radius auth ipsec enable 1
```

次に、RADIUS 認証サーバ インデックス 1 に対する IPSec サポートを無効にする例を示します。

```
(Cisco Controller) > config radius auth ipsec disable 1
```

関連コマンド

show radius acct statistics

config radius auth ipsec encryption

Cisco ワイヤレス LAN コントローラの認証サーバに対する IPSec 暗号化サポートを設定するには、**config radius auth ipsec encryption** コマンドを使用します。

config radius auth IPsec encryption {**256-aes** | **3des** | **aes** | **des**} *index*

構文の説明

256-aes	IPSec 256 AES 暗号化を有効にします。
3des	IPSec 3DES 暗号化を有効にします。
aes	IPSec AES 暗号化を有効にします。
des	IPSec DES 暗号化を有効にします。
index	RADIUS サーバ インデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	256-aes キーワードが追加されました。

次に、IPsec 3dec 暗号化の RADIUS 認証サーバ インデックス 3 を設定する例を示します。

```
(Cisco Controller) > config radius auth ipsec encryption 3des 3
```

関連コマンド

show radius acct statistics

config radius auth ipsec ike

Cisco ワイヤレス LAN コントローラのインターネット キー交換（IKE）を設定するには、**config radius auth IPsec ike** コマンドを使用します。

config radius auth ipsec ike {**auth-mode** {**pre-shared-key***index* {**ascii** | **hex** *shared-secret*} | **certificate** *index* } **dh-group** {**2048bit-group-14** | **group-1** | **group-2** | **group-5**} | **lifetime** *seconds* | **phase1** {**aggressive** | **main**}} *index*

構文の説明

auth-mode	IKE 認証方式を設定します。
pre-shared-key	IKE 認証方式の事前共有キーを設定します。
index	RADIUS サーバのインデックス（1 ～ 17）。
ascii	ASCII 形式の RADIUS IPSec IKE 秘密キーを設定します。
hex	16 進数形式の RADIUS IPSec IKE 秘密キーを設定します。
shared-secret	共有 RADIUS IPSec 秘密キーを設定します。
certificate	IKE 認証の証明書を設定します。
dh-group	IKE Diffe-Hellman グループを設定します。
2048bit-group-14	DH グループ 14（2048 ビット）を設定します。
group-1	DH グループ 1（768 ビット）を設定します。
group-2	DH グループ 2（1024 ビット）を設定します。
group-5	DH グループ 2（1024 ビット）を設定します。
lifetime	IKE ライフタイムを設定します。
seconds	IKE の有効期間（秒単位）。有効な範囲は 1800 ～ 57600 秒です。
phase1	IKE phase1 モードを設定します。
aggressive	アグレッシブ モードをイネーブルにします。
main	メイン モードをイネーブルにします。
index	RADIUS サーバ インデックス。

コマンド デフォルト

デフォルトでは、事前共有キーが IPSec セッションで使用され、IKE の有効期間は 28800 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、RADIUS 認証インデックス 1 の IKE の有効期間を 23 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth ipsec ike lifetime 23 1
```

関連コマンド

show radius acct statistics

config radius auth keywrap

Advanced Encryption Standard（AES）キー ラップを有効化および設定して、コントローラとRADIUS サーバの共有キーのセキュリティを強化するには、**config radius auth keywrap** コマンドを使用します。

config radius auth keywrap {**enable** | **disable** | **add** {**ascii** | **hex**} *kek mack* | **delete**} *index*

構文の説明

enable	AES キー ラップを有効にします。
disable	AES キー ラップを無効にします。
add	AES キー ラップの属性を設定します。
ascii	キー ラップを ASCII 形式で設定します。
hex	キー ラップを 16 進数表記で設定します。
kek	16 バイトの Key Encryption Key（KEK）。
mack	20 バイトの Message Authentication Code Key（MACK）。
delete	AES キー ラップの属性を削除します。
index	AES キー ラップを設定する RADIUS 認証サーバのインデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバの AES キー ラップを有効にする例を示します。

```
(Cisco Controller) > config radius auth keywrap enable
```

関連コマンド

show radius auth statistics

config radius auth mac-delimiter

RADIUS認証サーバに送信されるMACアドレスで使用されるデリミタを指定するには、**config radius auth mac-delimiter** コマンドを使用します。

config radius auth mac-delimiter {**colon** | **hyphen** | **single-hyphen** | **none**}

構文の説明

colon	デリミタをコロンに設定します（xx:xx:xx:xx:xx:xx など）。
hyphen	デリミタをハイフンに設定します（xx-xx-xx-xx-xx-xx など）。
single-hyphen	デリミタを単一ハイフンに設定します（xxxxxx-xxxxxx など）。
none	デリミタを無効にします（xxxxxxxxxxxx など）。

コマンド デフォルト

デフォルトのデリミタは、ハイフンです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、RADIUS 認証サーバに使用するデリミタ ハイフンを指定する例を示します。

```
(Cisco Controller) > config radius auth mac-delimiter hyphen
```

関連コマンド

show radius auth statistics

config radius auth management

管理ユーザのデフォルト RADIUS サーバを設定するには、**config radius auth management** コマンドを使用します。

config radius auth management *index* {**enable** | **disable**}

構文の説明

index	RADIUS サーバ インデックス。
enable	サーバを管理ユーザのデフォルトRADIUSサーバとして有効にします。
disable	サーバを管理ユーザのデフォルトRADIUSサーバとして無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、管理ユーザの RADIUS サーバを設定する例を示します。

```
(Cisco Controller) > config radius auth management 1 enable
```

関連コマンド

show radius acct statistics

config radius acct network

config radius auth mgmt-retransmit-timeout

config radius auth mgmt-retransmit-timeout

管理ユーザのデフォルト RADIUS サーバの再送信タイムアウトを設定するには、**config radius auth mgmt-retransmit-timeout** コマンドを使用します。

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

構文の説明

index	RADIUS サーバ インデックス。
retransmit-timeout	タイムアウト値。範囲は 1 ～ 30 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、管理ユーザのデフォルト RADIUS サーバの再送信タイムアウトを設定する例を示します。

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

関連コマンド

config radius auth management

config radius auth network

ネットワーク ユーザのデフォルト RADIUS サーバを設定するには、**config radius auth network** コマンドを使用します。

config radius auth network *index* {**enable** | **disable**}

構文の説明

index	RADIUS サーバ インデックス。
enable	サーバをネットワーク ユーザのデフォルト RADIUS サーバとして有効にします。
disable	サーバをネットワーク ユーザのデフォルト RADIUS サーバとして無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ネットワーク ユーザのデフォルト RADIUS サーバを設定する例を示します。

```
(Cisco Controller) > config radius auth network 1 enable
```

関連コマンド

show radius acct statistics

config radius acct network

config radius auth realm

RADIUS認証サーバでレルムを設定するには、**config radius auth realm** コマンドを使用します。

config radius auth realm {**add** | **delete**} *radius_index realm_string*

構文の説明

radius_server	RADIUS サーバ インデックス。範囲は 1 ～ 17 です。
add	RADIUS 認証サーバにレルムを追加します。
delete	RADIUS認証サーバからレルムを削除します。
realm_string	RADIUS 認証レルムに関連付けられた一意の文字列です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、RADIUS 認証サーバにレルムを追加する例を示します。

```
(Cisco Controller) > config radius auth realm add 3 test
```

config radius auth retransmit-timeout

Cisco ワイヤレス LAN コントローラの RADIUS 認証サーバのデフォルト送信タイムアウトを変更するには、**config radius auth retransmit-timeout** コマンドを使用します。

config radius auth retransmit-timeout *index timeout*

構文の説明

index	RADIUS サーバ インデックス。
timeout	秒単位での再送信間隔（2 ～ 30）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバの再送信タイムアウトを 5 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

関連コマンド

show radius auth statistics

config radius auth rfc3576

Cisco WLC の認証サーバに RADIUS RFC-3576 サポートを設定するには、**config radius auth rfc3576** コマンドを使用します。

config radius auth rfc3576 {**enable** | **disable**} *index*

構文の説明

enable	認証サーバの RFC-3576 サポートを有効にします。
disable	認証サーバの RFC-3576 サポートを無効にします。
index	RADIUS サーバ インデックス。

コマンド デフォルト

無効

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

RFC 3576 は RADIUS プロトコルに対する拡張で、ユーザ セッションの動的な変更を可能にします。RFC 3576 では、ユーザの切断およびユーザ セッションに適用される許可の変更がサポートされています。Disconnect メッセージはユーザ セッションをただちに終了させ、CoA メッセージはデータ フィルタなどのセッション認証属性を変更します。

次に、RADIUS 認証サーバに対する RADIUS RFC-3576 サポートを有効にする例を示します。

```
(Cisco Controller) > config radius auth rfc3576 enable 2
```

関連コマンド

show radius auth statistics

show radius summary

show radius rfc3576

config radius auth retransmit-timeout

RADIUS アカウンティング サーバの再送信タイムアウト値を設定するには、**config radius auth server-timeout** コマンドを使用します。

config radius auth retransmit-timeout *index timeout*

構文の説明

index	RADIUS サーバ インデックス。
timeout	タイムアウト値。範囲は 2 ～ 30 秒です。

コマンド デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバ インデックス 10 のサーバ タイムアウト値を 2 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

関連コマンド

show radius auth statistics

show radius summary

config radius aggressive-failover disabled

連続して 3 つのクライアントに応答しなかった RADIUS サーバをダウン（応答なし）としてマークするようにコントローラを設定するには、**config radius aggressive-failover disabled** コマンドを使用します。

config radius aggressive-failover disabled

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS サーバをダウンとしてマークするようにコントローラを設定する例を示します。

```
(Cisco Controller) > config radius aggressive-failover disabled
```

関連コマンド

show radius summary

config radius backward compatibility

Cisco ワイヤレス LAN コントローラの RADIUS 下位互換性を設定するには、**config radius backward compatibility** コマンドを使用します。

config radius backward compatibility {**enable** | **disable**}

構文の説明

enable	RADIUS ベンダー ID の下位互換性を有効にします。
disable	RADIUS ベンダー ID の下位互換性を無効にします。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 下位互換性の設定を有効にする例を示します。

```
(Cisco Controller) > config radius backward compatibility disable
```

関連コマンド

show radius summary

config radius callStationIdCase

Cisco WLC の RADIUS メッセージとして送信される callStationIdCase 情報を設定するには、**config radius callStationIdCase** コマンドを使用します。

config radius callStationIdCase {**legacy** | **lower** | **upper**}

構文の説明

legacy	レイヤ 2 認証用の呼出端末 ID を大文字で RADIUS に設定します。
lower	すべての呼出端末 ID を小文字で RADIUS に設定します。
upper	すべての呼出端末 ID を大文字で RADIUS に設定します。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、呼出端末 ID を小文字で送信する例を示します。

```
(Cisco Controller) > config radius callStationIdCase lower
```

関連コマンド

show radius summary

config radius callStationIdType

Cisco ワイヤレス LAN コントローラの RADIUS アカウンティング メッセージとして送信される着信端末 ID タイプ情報を設定するには、**config radius callStationIdType** コマンドを使用します。

config radius callStationIdType {**ap-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddr-only** | **ap-macaddr-ssid** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **ipaddr** | **macaddr** | **vlan-id**}

構文の説明

ipaddr	IP アドレスを使用する呼出端末 ID タイプを設定します（レイヤ 3 のみ）。
macaddr	システムの MAC アドレスを使用する呼出端末 ID タイプを設定します（レイヤ 2 およびレイヤ 3）。
ap-macaddr-only	アクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定します（レイヤ 2 およびレイヤ 3）。
ap-macaddr-ssid	*AP MAC address*:*SSID* の形式でアクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定します（レイヤ 2 およびレイヤ 3）。
ap-ethmac-only	アクセス ポイントのイーサネット MAC アドレスを使用する着信端末 ID タイプを設定します。
ap-ethmac-ssid	*AP Ethernet MAC address*:*SSID* の形式でアクセス ポイントのイーサネット MAC アドレスを使用する着信端末 ID タイプを設定します。
ap-group-name	AP グループ名を使用する呼出端末 ID タイプを設定します。AP が AP グループの一部でない場合、「default-group」が AP グループ名として使用されます。
flex-group-name	FlexConnect グループ名を使用する呼出端末 ID タイプを設定します。FlexConnect AP が FlexConnect グループの一部でない場合、システム MAC アドレスが呼出端末 ID として使用されます。
ap-name	アクセス ポイントの名前を使用する呼出端末 ID タイプを設定します。

ap-name-ssid	*AP name*:*SSID* の形式でアクセス ポイントの名前を使用する呼出端末 ID タイプを設定します。
ap-location	アクセス ポイントのロケーションを使用する呼出端末 ID タイプを設定します。
ap-mac-ssid-ap-group	着信端末 ID タイプを、<AP MAC address>:<SSID>:<AP Group> 形式に設定します。
vlan-id	システムの VLAN-ID を使用する呼出端末 ID タイプを設定します。
ap-label-address	呼出端末ID タイプを、アカウンティング メッセージの AP ラベルに印刷されている AP MAC アドレスに設定します。
ap-label-address-ssid	呼出端末 ID タイプを、AP MAC address:SSID 形式に設定します。

コマンド デフォルト

サーバの IP アドレス。

使用上のガイドライン

コントローラは、すべての認証パケットおよびアカウンティング パケットで RADIUS サーバに着信端末 ID 属性を送信します。着信端末 ID 属性を使用すると、属性値に基づいて、異なるグループにユーザを分類できます。コマンドは着信端末に対してのみ適用可能であり、発信端末には適用できません。

SSID のみを Calling-Station-ID として送信することはできません。SSID は、アクセス ポイント MAC アドレスまたはアクセス ポイント名のいずれかにのみ組み合わせることができます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
7.6	アクセス ポイントのイーサネット MAC アドレスをサポートするために **ap-ethmac-only** キーワードと **ap-ethmac-ssid** キーワードが追加されました。 **ap-label-address** および **ap-label-address-ssid** キーワードが追加されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、IP アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius callStationIdType ipaddr
```

次に、システムの MAC アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius callStationIdType macaddr
```

次に、アクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius callStationIdType ap-macaddr-only
```

config radius dns

DNS サーバから RADIUS IP 情報を取得するには、**config radius dns** コマンドを使用します。

config radius dns {**global** *port* {*ascii* | *hex*} *secret* | **query***url timeout* | **serverip** *ip_address* | **disable** | **enable**}

構文の説明

global	グローバル ポートと、DNS サーバから RADIUS IP 情報を取得する秘密キーを設定します。
port	認証用のポート番号。有効な範囲は 1 ～ 65535 です。すべての DNS サーバは同じ認証ポートを使用する必要があります。
ascii	ASCII に設定する必要のある共有秘密キーの形式。
hex	16 進数に設定する必要のある共有秘密キーの形式。
secret	RADIUS サーバのログイン秘密キー。
query	RADIUS サーバの完全修飾ドメイン名（FQDN）と、DNS タイムアウトを設定します。
url	RADIUS サーバの FQDN。FQDN は最大 63 文字の英数字（大文字と小文字を区別）で指定できます。
timeout	Cisco WLC がリクエストのタイムアウトを設定して再送信するまでの最大待機日数。指定できる範囲は 1 ～ 180 です。
serverip	DNS サーバの IP アドレスを設定します。
ip_address	DNS サーバの IP アドレス。
disable	RADIUS DNS 機能を無効にします。デフォルトでは、この機能はディセーブルになっています。
enable	Cisco WLC が DNS サーバから RADIUS IP 情報を取得できるようにします。 DNS クエリを有効にすると、スタティック設定よりも優先されます。つまり、DNS リストはスタティック AAA リストよりも優先されます。

コマンド デフォルト

グローバル ポートと、RADIUS IP 情報を取得する秘密キーを設定できません。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン アカウンティングポートは認証ポートから取得されます。すべてのDNSサーバは同じ秘密キーを使用する必要があります。

次に、Cisco WLC で RADIUS DNS 機能を有効にする例を示します。

```
(Cisco Controller) > config radius dns enable
```

config radius fallback-test

RADIUS サーバのフォールバック動作を設定するには、**config radius fallback-test** コマンドを入力します。

config radius fallback-test mode {**off** | **passive** | **active**} | **username** *username*} | {**interval** *interval*}

構文の説明

mode	モードを指定します。
off	RADIUS サーバのフォール バックを無効にします。
passive	関係のないプローブ メッセージを送信することなく、コントローラが使用可能なバックアップ サーバから（サーバ インデックスがより小さい）優先サーバに切り替えられます。コントローラは、しばらくの間非アクティブなすべてのサーバを無視し、あとで RADIUS メッセージの送信が必要になったときに再試行します。
active	RADIUS プローブ メッセージを送信し、非アクティブだったサーバがオンライン状態に戻っているかどうかを事前に確認した上で、コントローラが使用可能なバックアップ サーバから（サーバ インデックスがより小さい）優先サーバに切り替えられます。コントローラは、すべてのアクティブなRADIUS要求に対して、非アクティブなすべてのサーバを無視します。
username	ユーザ名を指定します。
username	ユーザ名。ユーザ名には、最大16文字の英数字を使用できます。
interval	プローブの間隔値を指定します。
interval	プローブの間隔。範囲は 180 ～ 3600 です。

コマンド デフォルト

デフォルトのプローブ間隔は 300 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、RADIUS アカウンティング サーバのフォールバック動作を無効にする例を示します。

```
(Cisco Controller) > config radius fallback-test mode off
```

次に、関係のないプローブ メッセージを送信することなく、コントローラが使用可能なバックアップ サーバから優先サーバに切り替えられるように設定する例を示します。

```
(Cisco Controller) > config radius fallback-test mode passive
```

次に、RADIUS プローブ メッセージを送信して、コントローラが使用可能なバックアップ サーバから優先サーバに切り替えられるように設定する例を示します。

```
(Cisco Controller) > config radius fallback-test mode active
```

関連コマンド

config advanced probe filter

config advanced probe limit

show advanced probe

show radius acct statistics

config radius ext-source-ports

RADIUS サーバで拡張送信元ポートのサポートを設定するには、**config radius ext-source-ports** コマンドを使用します。

config radius ext-source-ports { **enable** | **disable** }

構文の説明

enable	Radius 送信元ポート サポートを有効にします。
disable	Radius 送信元ポート サポートを無効にします。

コマンド デフォルト

なし

コマンド モード

Config

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、RADIUS サーバで拡張送信元ポートを有効にする例を示します。

```
config radius ext-source-ports enable
```

config radius acct retransmit-timeout

Cisco ワイヤレス LAN コントローラ の RADIUS アカウンティング サーバのデフォルト送信タイムアウトを変更するには、**config radius acct retransmit-timeout** コマンドを使用します。

config radius acct retransmit-timeout *index timeout*

構文の説明

index	RADIUS サーバ インデックス。
timeout	秒単位での再送信間隔（2 ～ 30）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、再送信間隔の再送信タイムアウト値を 5 秒に設定する例を示します。

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

関連コマンド

show radius acct statistics

config radius auth mgmt-retransmit-timeout

管理ユーザのデフォルト RADIUS サーバの再送信タイムアウトを設定するには、**config radius auth mgmt-retransmit-timeout** コマンドを使用します。

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

構文の説明

index	RADIUS サーバ インデックス。
retransmit-timeout	タイムアウト値。範囲は 1 ～ 30 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、管理ユーザのデフォルト RADIUS サーバの再送信タイムアウトを設定する例を示します。

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

関連コマンド

config radius auth management

config radius auth retransmit-timeout

Cisco ワイヤレス LAN コントローラの RADIUS 認証サーバのデフォルト送信タイムアウトを変更するには、**config radius auth retransmit-timeout** コマンドを使用します。

config radius auth retransmit-timeout *index timeout*

構文の説明

index	RADIUS サーバ インデックス。
timeout	秒単位での再送信間隔（2 ～ 30）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバの再送信タイムアウトを 5 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

関連コマンド

show radius auth statistics

config radius auth retransmit-timeout

RADIUS アカウンティング サーバの再送信タイムアウト値を設定するには、**config radius auth server-timeout** コマンドを使用します。

config radius auth retransmit-timeout *index timeout*

構文の説明

index	RADIUS サーバ インデックス。
timeout	タイムアウト値。範囲は 2 ～ 30 秒です。

コマンド デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバ インデックス 10 のサーバ タイムアウト値を 2 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

関連コマンド

show radius auth statistics

show radius summary

config redundancy interface address peer-service-port

ピア コントローラまたはスタンバイ コントローラのサービス ポートの IP アドレスとネットマスクを設定するには、**config redundancy interface address peer-service-port** コマンドを使用します。

config redundancy interface address peer-service-port *ip_address netmask*

構文の説明

ip_address	ピア サービス ポートの IP アドレス。
netmask	ピア サービス ポートのネットマスク。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

アクティブ コントローラからのみこのコマンドを設定できます。HA 機能の場合、サービス ポート設定はコントローラごとに行います。モードを HA から非 HA に変更すると（逆も同様）、これらの設定は失われます。

次に、ピア コントローラまたはスタンバイ コントローラのサービス ポート IP およびネットマスクを設定する例を示します。

```
(Cisco Controller) >config redundancy interface address peer-service-port 11.22.44.55
```

config redundancy mobilitymac

HAモビリティのMACアドレスを識別子として使用するように設定するには、**config redundancy mobilitymac** コマンドを使用します。

config redundancy mobilitymac *mac_address*

構文の説明

mac_address	アクティブ コントローラとスタンバイ コントローラのペアの識別子であるMACアドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

リリース8.0.110.0からそれ以降リリースにアップグレードすると、コマンドの設定は削除されます。アップグレード後に手動でモビリティ MAC アドレスを再設定する必要があります。

次に、HA モビリティの MAC アドレスを設定する例を示します。

```
(Cisco Controller) >config redundancy mobilitymac ff:ff:ff:ff:ff:ff
```

config redundancy mode

冗長性またはハイ アベイラビリティ（HA）を有効または無効にするには、**config redundancy mode** コマンドを使用します。

config redundancy mode {**sso** | **none**}

構文の説明

sso	ステートフル スイッチオーバー（SSO）またはホット スタンバイ冗長モードを有効にします。
none	冗長モードを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

冗長性を設定する前に、ローカルとピアの冗長管理 IP アドレスを設定する必要があります。

次に、冗長性を有効にする例を示します。

```
(Cisco Controller) >config redundancy mode sso
```

config redundancy peer-route

ピアまたはスタンバイ コントローラのルートを設定するには、**config redundancy peer-route** コマンドを使用します。

config redundancy peer-route {**add** | **delete**} *network_ip_address netmask gateway*

構文の説明

add	ネットワーク ルートを追加します。
delete	スタンバイ コントローラ固有のネットワーク ルートを削除します。
network_ip_address	ネットワーク IP アドレス。
netmask	ネットワークのサブネット マスク。
gateway	ルート ネットワークのゲートウェイの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

アクティブ コントローラからのみこのコマンドを設定できます。HA 機能の場合、サービス ポート設定はコントローラごとに行います。モードを HA から非 HA に変更すると（逆も同様）、これらの設定は失われます。

次に、ピアまたはスタンバイ コントローラのルートを設定する例を示します。

```
(Cisco Controller) >config redundancy peer-route add 10.1.1.0 255.255.255.0 10.1.1.1
```

config redundancy timer keep-alive-timer

キープアライブ タイムアウト値を設定するには、 **config redundancy timer keep-alive-timer** コマンドを使用します。

config redundancy timer keep-alive-timer *milliseconds*

構文の説明

milliseconds	ミリ秒単位のキープアライブ タイムアウト値。範囲は 100 ～ 400 ミリ秒です。

コマンド デフォルト

デフォルトのキープアライブ タイムアウト値は 100 ミリ秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、キープアライブ タイムアウト値を設定する例を示します。

```
(Cisco Controller) >config redundancy timer keep-alive-timer 200
```

config redundancy timer peer-search-timer

ピアの検索タイマーを設定するには、 **config redundancy timer peer-search-timer** コマンドを使用します。

config redundancy timer peer-search-timer *seconds*

構文の説明

seconds	秒単位のピアの検索タイマーの値。範囲は60～180秒です。

コマンド デフォルト

ピアの検索タイマーのデフォルト値は 120 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、起動ロールネゴシエーションのタイムアウト値（秒単位）を設定するために使用できます。

次に、冗長ピアの検索タイマーを設定する例を示します。

```
(Cisco Controller) >config redundancy timer peer-search-timer 100
```

config redundancy unit

Cisco WLC をプライマリまたはセカンダリ WLC として設定するには、 **config redundancy unit** コマンドを使用します。

config redundancy unit {**primary** | **secondary**}

構文の説明

primary	Cisco WLC をプライマリ WLC として設定します。
secondary	Cisco WLC をセカンダリ WLC として設定します。

コマンド デフォルト

プライマリ WLC がデフォルトの状態です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

セカンダリ WLC として設定された Cisco WLC は、有効な AP ライセンスのない HA の Stakable Unit（SKU）になります。

次に、Cisco WLC をプライマリ WLC として設定する例を示します。

```
(Cisco Controller) >config redundancy unit primary
```

config remote-lan

リモート LAN を設定するには、**config remote-lan** コマンドを使用します。

config remote-lan {**enable** | **disable**} {*remote-lan-id* | **all**}

構文の説明

enable	リモート LAN をイネーブルにします。
disable	リモート LAN をディセーブルにします。
remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
all	すべての無線 LAN を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 2 のリモート LAN をイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan enable 2
```

config remote-lan aaa-override

リモート LAN で AAA を介したユーザ ポリシー オーバーライドを設定するには、**config remote-lan aaa-override** コマンドを使用します。

config remote-lan aaa-override {**enable** | **disable**} *remote-lan-id*

構文の説明

enable	リモート LAN で AAA を介したユーザ ポリシー オーバーライドをイネーブルにします。
disable	リモート LAN で AAA を介したユーザ ポリシーオーバーライドをディセーブルにします。
remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、リモート LAN ID が 2 のリモート LAN で、AAA を介したユーザ ポリシー オーバーライドをイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan aaa-override enable 2
```

config remote-lan acl

リモート LAN のアクセス コントロール リスト（ACL）を指定するには、**config remote-lan acl** コマンドを使用します。

config remote-lan acl *remote-lan-id acl_name*

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
acl_name	ACL 名です。 （注） 使用可能な ACL を確認するには、**show acl summary**コマンドを使用します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID が 2 のリモート LAN に、ACL1 を指定する例を示します。

```
(Cisco Controller) >config remote-lan acl 2 ACL1
```

config remote-lan create

新しいリモート LAN 接続を設定するには、**config remote-lan create** コマンドを使用します。

config remote-lan create *remote-lan-id name*

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
name	リモート LAN の名前。有効な値は最大 32 文字の英数字です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LAN ID を 3 として、新しいリモート LAN、MyRemoteLAN を設定する例を示します。

```
(Cisco Controller) >config remote-lan create 3 MyRemoteLAN
```

config remote-lan custom-web

リモート LAN 用の Web 認証を設定するには、**config remote-lan custom-web** コマンドを使用します。

config remote-lan custom-web {**ext-webauth-url** *URL* } | **global** {**enable** | **disable**} | **login-page** *page-name* | **loginfailure-page** {*page-name* | **none**} | **logout-page** {*page-name* | **none**} | **webauth-type** {**internal** | **customized** | **external**}} *remote-lan-id*

構文の説明

ext-webauth-url	外部 Web 認証の URL を設定します。
URL	ログイン ページ用の Web 認証 URL。
global	リモート LAN のグローバル ステータスを設定します。
enable	リモート LAN のグローバル ステータスをイネーブルにします。
disable	リモート LAN のグローバル ステータスをディセーブルにします。
login-page	ログイン ページを設定します。
page-name	ログイン ページの名前。
none	ログイン ページを設定しません。
logout-page	ログアウト ページを設定します。
none	ログアウト ページを設定しません。
webauth-type	リモート LAN の Web 認証タイプを設定します。
internal	デフォルト ログイン ページを表示します。
customized	ダウンロードされたログイン ページを表示します。
external	外部サーバにあるログイン ページを表示します。
name	リモート LAN の名前。有効な値は最大 32 文字の英数字です。
remote-lan-id	リモート LAN の識別子。有効な値の範囲は 1 ～ 512 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config remote-lan custom-web コマンドを使用するときは、次のガイドラインに従ってください。

- 外部 Web 認証 URL を設定する場合は、次のようにしてください。
  - Web 認証または Web パススルー セキュリティがイネーブル状態であることを確認します。Web 認証を有効にするには、**config remote-lan security web-auth enable** コマンドを使用します。Web パススルーを有効にするには、**config remote-lan security web-passthrough enable** コマンドを使用します。
  - リモート LAN のグローバル ステータスがディセーブル状態になっていることを確認します。リモート LAN のグローバル ステータスをイネーブルにするには、**config remote-lan custom-web global disable** コマンドを使用します。
  - リモート LAN がディセーブル状態になっていることを確認します。リモート LAN を無効にするには、**config remote-lan disable** コマンドを使用します。
- リモート LAN 用の Web 認証タイプを設定する場合は、次のようにしてください。
  - カスタマイズされたログイン ページを設定する場合は、ログイン ページが設定されていることを確認します。ログイン ページを設定するには、**config remote-lan custom-web login-page** コマンドを使用します。
  - 外部ログイン ページを設定する場合は、外部 Web 認証が動作するように、事前認証 ACL を設定したことを確認します。

次に、ID 3 のリモート LAN に対して、外部 Web 認証 URL を設定する例を示します。

```
(Cisco Controller) >config remote-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 3
```

次に、ID 3 のリモート LAN のグローバル ステータスをイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan custom-web global enable 3
```

次に、ID 3 のリモート LAN に対して、ログイン ページを設定する例を示します。

```
(Cisco Controller) >config remote-lan custom-web login-page custompage1 3
```

次に、ID 3 のリモート LAN に対して、デフォルト ログイン ページで Web 認証タイプを設定する例を示します。

```
(Cisco Controller) >config remote-lan custom-web webauth-type internal 3
```

config remote-lan delete

リモート LAN 接続を削除するには、**config remote-lan delete** コマンドを使用します。

config remote-lan delete *remote-lan-id*

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 3 のリモート LAN を削除する例を示します。

```
(Cisco Controller) >config remote-lan delete 3
```

config remote-lan dhcp_server

リモート LAN の Dynamic Host Configuration Protocol（DHCP）サーバを設定するには、**config remote-lan dhcp_server** コマンドを使用します。

config remote-lan dhcp_server *remote-lan-id ip_address*

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
ip_addr	オーバーライド DHCP サーバの IPv4 アドレス。

コマンド デフォルト

0.0.0.0 がインターフェイスのデフォルト値として設定されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

次に、ID 3 のリモート LAN に対して、DHCP サーバを設定する例を示します。

```
(Cisco Controller) >config remote-lan dhcp_server 3 209.165.200.225
```

関連コマンド

show remote-lan

config remote-lan exclusionlist

リモート LAN の除外リスト タイムアウトを設定するには、**config remote-lan exclusionlist** コマンドを使用します。

config remote-lan exclusionlist *remote-lan-id* {*seconds* | **disabled** | **enabled**}

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
seconds	除外リスト タイムアウト（秒）。値 0 には、管理者のオーバーライドが必要です。
disabled	除外リストをディセーブルにします。
enabled	除外リストをイネーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 3 のリモート LAN で、除外リスト タイムアウトを 20 秒に設定する例を示します。

```
(Cisco Controller) >config remote-lan exclusionlist 3 20
```

config remote-lan interface

リモート LAN のインターフェイスを設定するには、**config remote-lan interface** コマンドを使用します。

config remote-lan interface *remote-lan-id interface_name*

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
interface_name	インターフェイス名。 （注） インターフェイス名は大文字にしないでください。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 3 のリモート LAN に対して、インターフェイス myinterface を設定する例を示します。

```
(Cisco Controller) >config remote-lan interface 3 myinterface
```

config remote-lan ldap

リモート LAN の LDAP サーバを設定するには、**config remote-lan ldap** コマンドを使用します。

config remote-lan ldap {**add** | **delete**} リモート *lan id* インデックス

構文の説明

add	設定済みの LDAP サーバ（最大 3 台）へのリンクを追加します。
delete	設定されている LDAP サーバへのリンクを削除します。
remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
index	LDAP サーバ インデックス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 3 のリモート LAN に対して、インデックス番号 10 の LDAP サーバを追加する例を示します。

```
(Cisco Controller) >config remote-lan ldap add 3 10
```

config remote-lan mac-filtering

リモート LAN で MAC フィルタリングを設定するには、**config remote-lan mac-filtering** コマンドを使用します。

config remote-lan mac-filtering {**enable** | **disable**} *remote-lan-id*

構文の説明

enable	リモート LAN で MAC フィルタリングをイネーブルにします。
disable	リモート LAN で MAC フィルタリングをディセーブルにします。
remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。

コマンド デフォルト

リモート LAN で MAC フィルタリングがイネーブルになります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 3 のリモート LAN で MAC フィルタリングをディセーブルにする例を示します。

```
(Cisco Controller) >config remote-lan mac-filtering disable 3
```

config remote-lan mab

AP ポート LAN クライアントのために MAC 認証バイパス（MAB）認証のサポートを設定するには、 **config remote-lan mab** コマンドを使用します。

config remote-lan mab {**enable** | **disable**} *remote-lan-id*

構文の説明

enable	MAB 認証のサポートを有効にします。
disable	MAB 認証のサポートを無効にします。
remote-lan-id	WLAN 識別子。有効な範囲は 1 ～ 512 です。

コマンド デフォルト

なし

コマンド モード

コントローラの設定

コマンド履歴

リリース	変更内容
8.4	このコマンドが導入されました。

例

次に、AP ポート LAN クライアントのために MAB 認証のサポートを有効にする例を示します。

```
(Cisco Controller) >config remote-lan mab enable 8
```

config remote-lan max-associated-clients

リモート LAN のクライアント接続の最大数を設定するには、**config remote-lan max-associated-clients** コマンドを使用します。

config remote-lan max-associated-clients *remote-lan-id max-clients*

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
max-clients	リモート LAN のクライアント接続の最大数を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 3 のリモート LAN に対して、10 のクライアント接続を設定する例を示します。

```
(Cisco Controller) >config remote-lan max-associated-clients 3 10
```

config remote-lan radius_server

リモート LAN で RADIUS サーバを設定するには、**config remote-lan radius_server** コマンドを使用します。

config remote-lan radius_server {**acct** {{**add** | **delete**} *server-index* | {**enable** | **disable**} | **interim-update** {*interval* | **enable** | **disable**}} | **auth** {{**add** | **delete**} *server-index* | {**enable** | **disable** }} | **overwrite-interface** {**enable** | **disable**}} *remote-lan-id*

構文の説明

acct	RADIUS アカウンティング サーバを設定します。
add	設定されている RADIUS サーバへのリンクを追加します。
delete	設定されている RADIUS サーバへのリンクを削除します。
remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
server-index	RADIUS サーバ インデックス。
enable	このリモート LAN の RADIUS アカウンティングをイネーブルにします。
disable	このリモート LAN の RADIUS アカウンティングをディセーブルにします。
interim-update	このリモート LAN の RADIUS アカウンティングをイネーブルにします。
interval	中間アカウンティングの間隔。範囲は 180 ～ 3600 秒です。
enable	中間アカウンティング アップデートをイネーブルにします。
disable	中間アカウンティングアップデートをディセーブルにします。
auth	RADIUS 認証サーバを設定します。
enable	このリモート LAN に対して RADIUS 認証をイネーブルにします。
disable	このリモート LAN に対して RADIUS 認証をディセーブルにします。

overwrite-interface	リモートLANのRADIUS動的インターフェイスを設定します。
enable	リモートLANのRADIUS動的インターフェイスをイネーブルにします。
disable	リモートLANのRADIUS動的インターフェイスをディセーブルにします。

コマンド デフォルト

暫定アップデート間隔は 600 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 3 のリモート LAN の RADIUS アカウンティングをイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan radius_server acct enable 3
```

config remote-lan security

リモート LAN のセキュリティ ポリシーを設定するには、**config remote-lan security** コマンドを使用します。

config remote-lan security {{**web-auth** {**enable** | **disable** | **acl** | **server-precedence**} *remote-lan-id* | {**web-passthrough** {**enable** | **disable** | **acl** | **email-input**} *remote-lan-id*}}

構文の説明

web-auth	Web 認証を指定します。
enable	Web 認証の設定をイネーブルにします。
disable	Web 認証の設定をディセーブルにします。
acl	アクセス コントロール リストを設定します。
server-precedence	Web 認証ユーザに対する認証サーバの優先順位を設定します。
remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
email-input	電子メール アドレスを使用して Web キャプティブ ポータルを設定します。
web-passthrough	認証不要の Web キャプティブ ポータルを設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.4	**802.1X** キーワードが追加されました。

次に、リモート LAN ID 1 のセキュリティ Web 認証ポリシーを設定する例を示します。

```
(Cisco Controller) >config remote-lan security web-auth enable 1
```

config remote-lan session-timeout

クライアント セッションのタイムアウトを設定するには、**config remote-lan session-timeout** コマンドを使用します。

config remote-lan session-timeout *remote-lan-id seconds*

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
seconds	タイムアウトまたはセッション時間（秒）。値 0 は、タイムアウトなしに相当します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 1 のリモート LAN で、クライアント セッション タイムアウトを 6000 秒に設定する例を示します。

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

config remote-lan webauth-exclude

リモート LAN の Web 認証の除外を設定するには、**config remote-lan webauth-exclude** コマンドを使用します。

config remote-lan webauth-exclude *remote-lan-id* {**enable** | **disable**}

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
enable	リモート LAN の Web 認証の除外をイネーブルにします。
disable	リモート LAN の Web 認証の除外をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 1 のリモート LAN で、Web 認証除外をイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan webauth-exclude 1 enable
```

config rf-profile band-select

RF プロファイルの帯域選択パラメータを設定するには、**config rf-profile band-select** コマンドを使用します。

config rf-profile band-select {**client-rssi** *rssi* | **cycle-count** *cycles* | **cycle-threshold** *value* | **expire** {**dual-band** *value* | **suppression** *value*} | **probe-response** {**enable** | **disable**}} *profile_name*

構文の説明

client-rssi	RF プロファイルに対して、クライアントの Received Signal Strength Indicator（RSSI）のしきい値を設定します。
rssi	プローブに応答するクライアントの RSSI の最小値。範囲は -20 ～ -90 dBm です。
cycle-count	RF プロファイルのプローブ サイクル カウントを設定します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。
cycles	サイクル カウントの値。値の範囲は 1 ～ 10 です。
cycle-threshold	新しいスキャン RF プロファイルの帯域選択サイクル時間のしきい値を設定します。この設定は、クライアントからの新しいプルーブ要求が新しいスキャン サイクルで送信される間の時間しきい値を決定します。
value	RF プロファイルのサイクルのしきい値。範囲は 1 ～ 1000 ミリ秒です。
expire	帯域選択に対するクライアントの有効期限を設定します。
dual-band	既知のデュアルバンド クライアントを除去する有効期限を設定します。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
value	デュアルバンドの値。範囲は 10 ～ 300 秒です。
suppression	既知の 802.11b/g クライアントを除去する有効期限を設定します。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
value	抑制の値。範囲は 10 ～ 200 秒です。
probe-response	RF プロファイルのプローブ応答を設定します。
enable	RF プロファイルに対して、2.4 GHz 帯域で動作しているクライアントのプローブ応答抑制をイネーブルにします。
disable	RF プロファイルに対して、2.4 GHz 帯域で動作しているクライアントのプローブ応答抑制をディセーブルにします。

profile name	RF プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

クライアント RSSI のデフォルト値は -80 dBm です。

デフォルトのサイクル回数は 2 です。

デフォルトのサイクル閾値は 200 ミリ秒です。

デュアルバンドの有効期限のデフォルト値は 60 秒です。

抑制の有効期限のデフォルト値は 20 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

WLAN で帯域選択を有効にすると、アクセス ポイントによって 2.4 GHz でのクライアント プローブが抑制され、デュアル バンド クライアントが 5 Ghz スペクトルに移動されます。帯域選択アルゴリズムによるデュアルバンドクライアントの誘導は、同じアクセスポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。

次に、クライアント RSSI を設定する例を示します。

```
(Cisco Controller) >config rf-profile band-select client-rssi -70
```

config rf-profile channel

RF プロファイルの DCA を設定するには、**config rf-profile channel** コマンドを使用します。

config rf-profile channel {**add** *chan profile name* | **delete** *chan profile name* | **foreign** {**enable** | **disable**} *profile name* | **chan-width** {**20** | **40** | **80**} *profile name*}

構文の説明

add	RF プロファイルの DCA チャネル リストにチャネルを追加します。
delete	RF プロファイルの DCA チャネル リストからチャネルを削除します。
foreign	RF プロファイルの DCA 外部 AP の寄与を設定します。
chan-width	RF プロファイルの DCA チャネル幅を設定します。
chan	チャネル番号を指定します。
profile name	RF プロファイルの名前を指定します。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。
enable	外部 AP 干渉を有効にします。
disable	外部 AP 干渉を無効にします。
{**20** | **40** | **80**}	RF プロファイルの DCA チャネル幅を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、RF プロファイルの DCA チャネル リストにチャネルを追加する例を示します。

```
(Cisco Controller) >config rf-profile channel add 40 admin1
```

次に、RF プロファイルの DCA チャネル幅を設定する例を示します。

```
(Cisco Controller) >config rf-profile channel chan-width 40 admin1
```

config rf-profile client-trap-threshold

アクセスポイントに関連付けられるクライアント数のしきい値を設定するには（このしきい値を超えると、SNMP トラップがコントローラに送信される）、**config rf-profile client-trap-threshold** コマンドを使用します。

config rf-profile client-trap-threshold *threshold profile_name*

構文の説明

threshold	アクセスポイントに関連付けられるクライアント数のしきい値。このしきい値を超えると、SNMP トラップがコントローラに送信されます。範囲は 0 ～ 200 です。トラップは、しきい値がゼロに設定されている場合はディセーブルです。
profile_name	RF プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントに関連付けられているクライアント数のしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile client-trap-threshold 150
```

config rf-profile create

RF プロファイルを作成するには、**config rf-profile create** コマンドを使用します。

config rf-profile create {**802.11a** | **802.11b/g**} *profile-name*

構文の説明

802.11a	2.4GHz 帯域の RF プロファイルを設定します。
802.11b/g	5GHz 帯域の RF プロファイルを設定します。
profile-name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、新しい RF プロファイルを作成する例を示します。

```
(Cisco Controller) >config rf-profile create 802.11a RFtestgroup1
```

config rf-profile fra client-aware

RF プロファイルのクライアント認識 FRA 機能を設定するには、**config rf-profile fra client-aware** コマンドを使用します。

config rf-profile fra client-aware {**client-reset** *percent rf-profile-name* | **client-select** *percent rf-profile-name* | **disable** *rf-profile-name* | **enable** *rf-profile-name*}

構文の説明

client-reset	無線をモニタ モードに戻すための RF プロファイルの AP 使用率のしきい値を設定します。
percent	0 ～ 100 までの使用率の値。デフォルト値は 5% です。
rf-profile-name	RF プロファイルの名前。
client-select	無線を 5GHz に切り替えるための RF プロファイル使用率のしきい値を設定します。
percent	0 ～ 100 までの使用率の値。デフォルト値は 50 % です。
disable	RF プロファイルのクライアント認識 FRA 機能を無効にします。
enable	RF プロファイルのクライアント認識 FRA 機能を有効にします。

コマンド デフォルト

client-select および client-reset のデフォルトのパーセント値は、それぞれ 50% および 5% です。

コマンド履歴

リリース	変更内容
8.5	このコマンドが導入されました。

次に、冗長デュアルバンド無線を 5 GHz クライアント サーバの役割からモニタ モードに戻すための RF プロファイル使用率のしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

次に、冗長デュアルバンド無線をモニタ モードから 5 GHz クライアント サーバの役割に切り替えるための RF プロファイル使用率のしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

次に、RF プロファイルのクライアント認識 FRA 機能を無効にする例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

次に、RF プロファイルのクライアント認識 FRA 機能を有効にする例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```

config rf-profile data-rates

RF プロファイルのデータ レートを設定するには、**config rf-profile data-rates** コマンドを使用します。

config rf-profile data-rates {**802.11a** | **802.11b** } {**disabled** | **mandatory** | **supported**} *data-rate profile-name*

構文の説明

802.11a	RF プロファイルの無線ポリシーとして 802.11a を指定します。
802.11b	RF プロファイルの無線ポリシーとして 802.11b を指定します。
disabled	レートをディセーブルにします。
mandatory	レートを必須に設定します。
supported	レートをサポートに設定します。
data-rate	802.11 動作レート（1*、2*、5.5*、6、9、11*、12、18、24、36、48、および 54）。* は、802.11b のみのレートであることを示します。
profile-name	RF プロファイルの名前。

コマンド デフォルト

RF プロファイルのデフォルトのデータ レートは、コントローラ システムのデフォルトであるグローバル データ レート設定から取得されます。たとえば、RF プロファイルの無線ポリシーが 802.11a にマッピングされると、グローバル 802.11a データ レートは、作成時に RF プロファイルにコピーされます。

このコマンドで設定したデータ レートは、クライアントと Cisco ワイヤレス LAN コントローラとの間でネゴシエートされます。データ レートが mandatory に設定されている場合、クライアントはネットワークを使用するためにこのデータ レートをサポートする必要があります。Cisco ワイヤレス LAN コントローラでデータ レートが supported に設定されている場合、アソシエートされているその他のクライアントのうち、このレートをサポートするクライアントも、このレートを使用して Cisco Lightweight アクセス ポイントと通信できます。アソシエートするために、クライアントが supported とマークされているすべてのレートを使用できる必要はありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、12 Mbps の必須レートで RF プロファイルの 802.11b 伝送を設定する例を示します。

```
(Cisco Controller) >config rf-profile 802.11b data-rates mandatory 12 RFGroup1
```

config rf-profile delete

RF プロファイルを削除するには、**config rf-profile delete** コマンドを使用します。

config rf-profile delete *profile-name*

構文の説明

profile-name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RF プロファイルを削除する例を示します。

```
(Cisco Controller) >config rf-profile delete RFGroup1
```

config rf-profile description

RF プロファイルの説明を入力するには、**config rf-profile description** コマンドを使用します。

config rf-profile description *description profile-name*

構文の説明

description	RF プロファイルの説明。
profile-name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RF プロファイルに説明を追加する例を示します。

```
(Cisco Controller) >config rf-profile description This is a demo desciption RFGroup1
```

config rf-profile load-balancing

RF プロファイルのロード バランシングを設定するには、**config rf-profile load-balancing** コマンドを使用します。

config rf-profile load-balancing {**window** *clients* | **denial** *value*} *profile_name*

構文の説明

window	RF プロファイルのロード バランシング用のクライアント・ウィンドウを設定します。
clients	アクセス ポイントとのクライアント アソシエーションを制限するクライアント ウィンドウ サイズ。指定できる範囲は 0 ～ 20 です。デフォルト値は 5 です。 このウィンドウ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。 ロード バランシング ウィンドウ + 最も負荷が低いアクセス ポイント上のクライアント アソシエーション数 = ロード バランシングしきい値 クライアント アソシエーションの数がこの閾値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数が閾値を下回るアクセスポイントだけとなります。このウィンドウでは、スティッキ クライアントをアソシエート解除することもできます。
denial	RFプロファイルのロードバランシング用にクライアントの拒否数を設定します。
value	ロード バランシング中のアソシエーション拒否の最大数。値の範囲は 1 ～ 10 です。デフォルト値は 3 です。 クライアントをワイヤレス ネットワークに関連付けようとする場合、クライアントは、アクセス ポイントにアソシエーション要求を送信します。アクセス ポイントが過負荷になり、ロード バランシングがコントローラ上でイネーブルな場合、アクセス ポイントはアソシエーション要求に対して拒否を送信します。他のアクセス ポイントがクライアントの範囲に含まれていない場合、クライアントは同じアクセス ポイントへの関連付けを再試行します。拒否の最大数に到達した後、クライアントが関連付けられます。AP に関連付けられる前のクライアントからアクセス ポイントへのアソシエーション試行は、アソシエーションのシーケンスと呼ばれます。デフォルトは 3 です。
profile_name	RF プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RF プロファイルのクライアント ウィンドウ サイズを設定する例を示します。

```
(Cisco Controller) >config rf-profile load-balancing window 15
```

config rf-profile max-clients

RFプロファイルのアクセスポイントごとのクライアント接続の最大数を設定するには、**config rf-profile max-clients** コマンドを使用します。

config rf-profile max-clients *clients*

構文の説明

clients	RF プロファイルのアクセス ポイントあたりのクライアント接続の最大数。指定できる範囲は 1 ～ 200 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

クライアントの高密度領域にあるアクセスポイント、または高帯域幅のビデオまたはミッション クリティカルな音声アプリケーションを提供しているアクセス ポイント上でクライアントの最大数を設定するには、このコマンドを使用します。

次に、クライアントの最大数を 50 に設定する例を示します。

```
(Cisco Controller) >config rf-profile max-clients 50
```

config rf-profile multicast data-rate

RF プロファイルの最小マルチキャスト データ レートを設定するには、**config rf-profile multicast data-rate** コマンドを使用します。

config rf-profile multicast data-rate *value profile_name*

構文の説明

value	RF プロファイルの最小マルチキャスト データ レート。オプションは 6、9、12、18、24、36、48、54 です。アクセス ポイントで動的なデータ レートを調整する場合は 0 を入力します。
profile_name	RF プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

RF プロファイルの最小マルチキャスト データ レートは 0 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RF プロファイルのマルチキャスト データ レートを設定する例を示します。

```
(Cisco Controller) >config rf-profile multicast data-rate 24
```

config rf-profile out-of-box

新しく設置したアクセス ポイントから構成されるアウトオブボックス AP グループを作成するには、**config rf-profile out-of-box** コマンドを使用します。

config rf-profile out-of-box {**enable** | **disable**}

構文の説明

enable アウトオブボックス AP グループの作成をイネーブルにします。このコマンドをイネーブルにすると、次の動作が発生します。

- デフォルト AP グループに含まれ、新しくインストールしたアクセス ポイントは、アウトオブボックス AP グループの一部となります。その無線はオフに切り替えられ、新しいアクセス ポイントによって生じる RF の不安定が解消されます。
- グループ名を持たないすべてのアクセス ポイントは、アウトオブボックス AP グループの一部になります。
- 特別な RF プロファイルは 802.11 帯域ごとに作成されます。これらの RF プロファイルには、既存のすべての RF パラメータのデフォルト設定、および追加の新しい設定があります。

disable アウトオブボックス AP グループをディセーブルにします。この機能をディセーブルにすると、アウトオブボックス AP グループへの新しい AP サブスクリプションだけが停止します。アウトオブザボックス AP グループへサブスクライブされたすべての AP が、この AP グループに残ります。ネットワーク コンバージェンス時に、デフォルト グループまたはカスタム AP グループに AP を移動できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

アウトオブザボックス AP がコントローラに最初に関連付けられるとき、その AP は特別な AP グループにリダイレクトされ、この AP グループに適用可能な RF プロファイルは、AP の無線管理状態の設定を制御します。ネットワーク コンバージェンス時に、デフォルト グループまたはカスタム グループに AP を移動できます。

次に、アウトオブボックス AP グループの作成をイネーブルにする例を示します。

```
(Cisco Controller) >config rf-profile out-of-box enable
```

config rf-profile rx-sop threshold

802.11 帯域ごとに高、中、低の Rx SOP しきい値を設定するには、**config rf-profile rx-sop threshold** コマンドを入力します。

config rf-profile rx-sop threshold {**high** | **medium** | **low** | **auto**} *profile_name*

構文の説明

high	RF プロファイルの高 Rx SOP しきい値を設定します。
medium	RF プロファイルの中 Rx SOP しきい値を設定します。
low	RF プロファイルの低 Rx SOP しきい値を設定します。
auto	RF プロファイルの自動 Rx SOP しきい値を設定します。auto を選択すると、アクセス ポイントが最適な Rx SOP しきい値を決定します。
profile_name	Rx SOP しきい値を設定する RF プロファイル。

コマンド デフォルト

デフォルトの Rx SOP しきい値オプションは auto です。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、RF プロファイルの高 Rx SOP しきい値を設定する例を示します。

```
(Cisco Controller) > config 802.11 rx-sop threshold high T1a
```

config rf-profile trap-threshold

RF プロファイルのトラップしきい値を設定するには、**config rf-profile trap-threshold** コマンドを使用します。

config rf-profile trap-threshold {**clients** *clients profile name* | **interference** *percent profile name* | **noise** *dBm profile name* | **utilization** *percent profile name*}

構文の説明

clients	RF プロファイルのクライアントのトラップしきい値を設定します。
clients	トラップ用のアクセス ポイントの無線のクライアント数は 1 ～ 200 です。デフォルトは 12 クライアントです。
profile name	RF プロファイルの名前を指定します。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。
interference	RF プロファイルの干渉のトラップしきい値を設定します。
percent	トラップ用の干渉しきい値の割合は 0 ～ 100% です。デフォルトは 10 % です。
noise	RF プロファイルのノイズのトラップしきい値を設定します。
dBm	トラップ用のノイズしきい値のレベルは -127 ～ 0 dBm です。デフォルトは -17 dBm です。
utilization	RF プロファイルの使用率のトラップしきい値を設定します。
percent	アクセスポイントしきい値で使用されるトラップ用の帯域幅の割合は 0 ～ 100% です。デフォルトは 80 % です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、RF プロファイルのクライアントのトラップしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile trap-threshold clients 50 admin1
```

config rf-profile tx-power-control-thresh-v1

RF プロファイルに Transmit Power Control バージョン 1（TPCv1）を設定するには、**config rf-profile tx-power-control-thresh-v1** コマンドを使用します。

config rf-profile tx-power-control-thresh-v1 *tpc-threshold profile_name*

構文の説明

tpc-threshold	TPC しきい値。
profile-name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RF プロファイルの TPCv1 を設定する例を示します。

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v1 RFGroup1
```

config rf-profile tx-power-control-thresh-v2

RF プロファイルに Transmit Power Control バージョン 2（TPCv2）を設定するには、**config rf-profile tx-power-control-thresh-v2** コマンドを使用します。

config rf-profile tx-power-control-thresh-v2 *tpc-threshold profile-name*

構文の説明

tpc-threshold	TPC しきい値。
profile-name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RF プロファイルの TPCv2 を設定する例を示します。

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v2 RFGroup1
```

config rf-profile tx-power-max

RF プロファイルに最大自動 RF を設定するには、**config rf-profile tx-power-max** コマンドを使用します。

config rf-profile *tx-power-max profile-name*

構文の説明

tx-power-max	最大自動 RF TX 電力。
profile-name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RF プロファイルの tx-power-max を設定する例を示します。

```
(Cisco Controller) >config rf-profile tx-power-max RFGroup1
```

config rf-profile tx-power-min

RF プロファイルに最小自動 RF を設定するには、**config rf-profile tx-power-min** コマンドを使用します。

config rf-profile tx-power-min *tx-power-min profile-name*

構文の説明

tx-power-min	最小自動 RF TX 電力。
profile-name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RF プロファイルの tx-power-min を設定する例を示します。

```
(Cisco Controller) >config rf-profile tx-power-min RFGroup1
```

config rogue ap timeout

不正なアクセスポイントおよびクライアントのエントリが期限切れとなり、リストから削除されるまでの秒数を指定するには、**config rogue ap timeout** コマンドを使用します。

config rogue ap timeout *seconds*

構文の説明

seconds	240 ～ 3600 秒までの値。デフォルト値は 1200 秒です。

コマンド デフォルト

不正なアクセスポイントおよびクライアントのエントリが期限切れとなるまでのデフォルトの秒数は、1200 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、不正アクセス ポイントとクライアント リストのエントリの有効期限を 2400 秒に設定する例を示します。

```
(Cisco Controller) > config rogue ap timeout 2400
```

関連コマンド

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue adhoc

独立型基本サービス セット（IBSS またはアドホック）の不正なアクセス ポイントのステータスをグローバルまたは個別に設定するには、**config rogue adhoc** コマンドを使用します。

config rogue adhoc {**enable** | **disable** | **external** *rogue_MAC* | **alert** {*rogue_MAC* | **all**} | **auto-contain** [*monitor_ap*] | **contain** *rogue_MAC 1234_aps*| }

config rogue adhoc {**delete** {**all** | **mac-address** *mac-address*} | **classify** {**friendly state** {**external** | **internal**} *mac-address* | **malicious state** {**alert** | **contain**} *mac-address* | **unclassified state** {**alert** | **contain** } *mac-address*}

構文の説明

enable	アドホックの不正の検出とレポートをグローバルに有効にします。
disable	アドホックの不正の検出とレポートをグローバルに無効にします。
external	ネットワークの外側にあり、WLAN のセキュリティに脅威を与えない不正アクセス ポイントの外部状態を設定します。コントローラはこの不正なアクセス ポイントの存在を認識しています。
rogue_MAC	アドホックの不正なアクセスポイントのMACアドレス。
alert	アドホックの不正を検出すると SMNP トラップを生成し、システム管理者に即座にアラートを発信し必要な措置を促します。
all	すべてのアドホックの不正なアクセス ポイントに関するアラートを有効にします。
auto-contain	コントローラによって検出されたすべての有線アドホックの不正が含まれます。
monitor_ap	（任意）アドホックの不正なアクセス ポイントの IP アドレス。
contain	加害デバイスを阻止し、その信号が正規クライアントを阻害しないようにします。
1234_aps	アドホックの不正なアクセス ポイントをアクティブに阻止するために割り当てられた、シスコのアクセスポイントの最大数（1～4）。

delete	アドホックの不正なアクセス ポイントを削除します。
all	すべてのアドホックの不正なアクセス ポイントを削除します。
mac-address	指定したMACアドレスがあるアドホックの不正なアクセス ポイントを削除します。
mac-address	アドホックの不正なアクセスポイントのMACアドレス。
classify	アドホックの不正なアクセス ポイントの分類を設定します。
friendly state	アドホックの不正なアクセス ポイントを危険性のないアクセスポイントとして分類します。
internal	ネットワークの内側にあり、WLAN のセキュリティに脅威を与えない不正アクセス ポイントのアラート状態を設定します。コントローラはこの不正なアクセス ポイントを信頼します。
malicious state	アドホックの不正なアクセス ポイントを悪意のあるアクセス ポイントとして分類します。
alert	ネイバー リストにない、またはユーザが設定した危険性のないMACのリストに記載されていない不正アクセス ポイントのアラート状態を設定します。コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。
contain	不正アクセス ポイントを contain の状態に設定します。コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
unclassified state	アドホックの不正なアクセス ポイントを未分類のアクセス ポイントとして分類します。

コマンド デフォルト

このコマンドのデフォルトは**enabled**であり、**alert**に設定されます。自動阻止のデフォルトは、**disabled**です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

コントローラは、すべての近隣のアクセス ポイントを継続的に監視し、不正なアクセス ポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラが不正なアクセス ポイントを検出すると、不正ロケーション検出プロトコル（RLDP）を使用して不正なアクセス ポイントが有線ネットワークに接続されているかどうかを確認します。

（注） RLDPは、シスコのAtonomous不正アクセス ポイントではサポートされていません。これらのアクセスポイントは、RLDPクライアントによって送信されたDHCP検出要求をドロップします。また不正なアクセスポイントチャネルが動的周波数選択（DFS）を必要とする場合、RLDPはサポートされません。

containment コマンドのいずれかを入力すると、次の警告が表示されます。

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

産業科学医療（ISM）帯域の2.4 GHz-および5 GHzの周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

不正なアクセス ポイントを阻止せずにそのアクセス ポイントを監視するには、*monitor_ap* 引数を使用して **auto-contain** コマンドを入力します。コントローラで検出されたすべてのアドホックの不正な有線アクセス ポイントを自動的に阻止するには、オプションの *monitor_ap* を使用せずに **auto-contain** コマンドを入力します。

次に、アドホックの不正の検出とレポートを有効にする例を示します。

```
(Cisco Controller) > config rogue adhoc enable
```

次に、すべてのアドホックの不正なアクセス ポイントに対するアラートを有効にする例を示します。

```
(Cisco Controller) > config rogue adhoc alert all
```

次に、アドホックの不正なアクセス ポイントを危険性なしとして分類し、外部状態を設定する例を示します。

```
(Cisco Controller) > config rogue adhoc classify friendly state internal 11:11:11:11:11:11
```

関連コマンド

config rogue auto-contain level

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap classify

不正なアクセス ポイントのステータスを分類するには、**config rogue ap classify** コマンドを使用します。

config rogue ap classify {**friendly state** {**internal** | **external**} *ap_mac*}

config rogue ap classify {**malicious** | **unclassified**} **state** {**alert** | **contain**}*ap_mac*

構文の説明

friendly	不正なアクセス ポイントを危険性なしとして分類します。
state	分類への応答を指定します。
internal	この不正なアクセス ポイントを信頼するようにコントローラを設定します。
external	このアクセス ポイントの存在を認めるようにコントローラを設定します。
ap_mac	不正なアクセス ポイントの MAC アドレス。
malicious	不正なアクセス ポイントを潜在的悪意として分類します。
unclassified	不正なアクセス ポイントを不明として分類します。
alert	システム管理者に即座にアラートを発信し、必要な措置を促すようにコントローラを設定します。
contain	危険性のあるデバイスを阻止して、そのデバイスの信号が認証されたクライアントに干渉しないようにコントローラを設定します。

コマンド デフォルト

これらのコマンドは、デフォルトでは無効になっています。したがって、すべての不明なアクセス ポイントは、デフォルトでは**unclassified**として分類されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

現在の状態が Contain の場合、不正なアクセス ポイントは Unclassified クラスに移動できません。

いずれかの containment コマンドを入力すると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療（ISM）帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、不正なアクセス ポイントを危険性なしとして分類し、信頼できるようにする例を示します。

```
(Cisco Controller) > config rogue ap classify friendly state internal 11:11:11:11:11:11
```

次に、不正なアクセス ポイントを悪意として分類し、アラートを送信する例を示します。

```
(Cisco Controller) > config rogue ap classify malicious state alert 11:11:11:11:11:11
```

次に、不正なアクセス ポイントを未分類として分類し、阻止する例を示します。

```
(Cisco Controller) > config rogue ap classify unclassified state contain 11:11:11:11:11:11
```

関連コマンド

config rogue adhoc

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap friendly

新しい危険性のないアクセス ポイント エントリを危険性のない MAC アドレスのリストに追加したり、リストから既存の危険性のないアクセスポイントエントリを削除したりするには、**config rogue ap friendly** コマンドを入力します。

config rogue ap friendly {**add** | **delete**} *ap_mac*

構文の説明

add	危険性のない MAC アドレス リストからこの不正なアクセス ポイントを追加します。
delete	危険性のない MAC アドレス リストからこの不正なアクセス ポイントを削除します。
ap_mac	追加または削除する不正なアクセス ポイントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレスが 11:11:11:11:11:11 の新しい危険性のないアクセス ポイントを危険性のない MAC アドレス リストに追加する例を示します。

```
(Cisco Controller) > config rogue ap friendly add 11:11:11:11:11:11
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap rldp

Rogue Location Discovery Protocol（RLDP）を有効化、無効化、または開始するには、**config rogue ap rldp** コマンドを使用します。

config rogue ap rldp enable {**alarm-only** | **auto-contain**} [*monitor_ap_only*]

config rogue ap rldp initiate *rogue_mac_address*

config rogue ap rldp disable

構文の説明

alarm-only	オプションの引数 *monitor_ap_only* を使用せずに入力すると、すべてのアクセス ポイントで RLDP が有効になります。
auto-contain	オプションの引数 *monitor_ap_only* を使用せずに入力すると、すべての不正なアクセス ポイントが自動的に阻止されます。
monitor_ap_only	（任意）指定した監視アクセス ポイントだけで RLDP を有効にするか（**alarm-only**キーワードを使用した場合）、または自動阻止を有効にします（**auto-contain**キーワードを使用した場合）。
initiate	特定の不正なアクセス ポイントで RLDP を開始します。
rogue_mac_address	特定の不正なアクセス ポイントの MAC アドレス。
disable	すべてのアクセス ポイントで RLDP を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

いずれかの containment コマンドを入力すると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療（ISM）帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、すべてのアクセス ポイントで RLDP を有効にする例を示します。

```
(Cisco Controller) > config rogue ap rldp enable alarm-only
```

次に、監視モード アクセス ポイント ap_1 で RLDP を有効にする例を示します。

```
(Cisco Controller) > config rogue ap rldp enable alarm-only ap_1
```

次に、MAC アドレスが 123.456.789.000 の不正なアクセス ポイントで RLDP を開始する例を示します。

```
(Cisco Controller) > config rogue ap rldp initiate 123.456.789.000
```

次に、すべてのアクセス ポイントで RLDP を無効にする例を示します。

```
(Cisco Controller) > config rogue ap rldp disable
```

関連コマンド

config rogue adhoc
config rogue ap classify
config rogue ap friendly
config rogue ap ssid
config rogue ap timeout
config rogue ap valid-client
config rogue client
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue ap ssid

アラームだけを生成するか、またはネットワークの Service Set Identifier（SSID）をアドバタイズしている不正なアクセス ポイントを阻止するには、**config rogue ap ssid** コマンドを使用します。

config rogue ap ssid {**alarm** | **auto-contain**}

構文の説明

alarm	不正なアクセス ポイントがネットワークの SSID をアドバタイズしていることを検出すると、アラームだけを生成します。
auto-contain	ネットワークの SSID をアドバタイズしている不正なアクセス ポイントを自動的に阻止します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

いずれかの containment コマンドを入力すると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療（ISM）帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、ネットワークの SSID をアドバタイズしている不正なアクセス ポイントを自動的に阻止する例を示します。

```
(Cisco Controller) > config rogue ap ssid auto-contain
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap timeout

不正なアクセス ポイントおよびクライアントのエントリが期限切れとなり、リストから削除されるまでの秒数を指定するには、**config rogue ap timeout** コマンドを使用します。

config rogue ap timeout *seconds*

構文の説明

seconds	240 ～ 3600 秒までの値。デフォルト値は 1200 秒です。

コマンド デフォルト

不正なアクセス ポイントおよびクライアントのエントリが期限切れとなるまでのデフォルトの秒数は、1200 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、不正アクセス ポイントとクライアント リストのエントリの有効期限を 2400 秒に設定する例を示します。

```
(Cisco Controller) > config rogue ap timeout 2400
```

関連コマンド

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue auto-contain level

不正の自動阻止レベルを設定するには、**config rogue auto-contain level** コマンドを使用します。

config rogue auto-contain level *level*［**monitor_ap_only**］

構文の説明

level	1 ～ 4 の範囲の不正の自動阻止レベル。 0 の値を入力すると、Cisco WLC が自動阻止に使用する AP の数を自動的に選択できるようになります。コントローラは、有効な阻止のために必要な AP の数を RSSI に基づいて選択します。 （注） 自動阻止ポリシーによって不正な AP が阻止状態に移行された際に、最大 4 つの AP を自動阻止に使用できます。
monitor_ap_only	（任意）監視 AP モードのみを使用して自動阻止を設定します。

コマンド デフォルト

デフォルトの自動阻止レベルは 1 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラは、すべての近隣のアクセス ポイントを継続的に監視し、不正なアクセス ポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラは、不正なアクセス ポイントを検出すると、設定済み自動阻止ポリシーを使用して自動阻止を開始します。自動阻止を開始するポリシーは、ワイヤ上の不正（RLDP または Rogue Detector AP によって検出）、管理対象 SSID を使用した不正、不正な AP の有効なクライアント、およびアドホック不正です。

このテーブルは、各阻止レベルに関連付けられている RSSI 値を示します。

表 *7:* 各阻止レベルに関連付けられている *RSSI*

自動阻止レベル	RSSI
1	0 ~ –55 dBm
2	–75 ～ –55 dBm
3	–85 ～ –75 dBm
4	–85 dBm 未満

（注） RLDPは、シスコのAtonomous不正アクセスポイントではサポートされていません。これらのアクセスポイントは、RLDPクライアントによって送信されたDHCP検出要求をドロップします。また不正なアクセスポイントチャネルが動的周波数選択（DFS）を必要とする場合、RLDPはサポートされません。

containment コマンドのいずれかを入力すると、次の警告が表示されます。

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

産業科学医療（ISM）帯域の 2.4 GHz および 5 GHz の周波数は一般に公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、自動阻止のレベルを 3 に設定する例を示します。

```
(Cisco Controller) > config rogue auto-contain level 3
```

関連コマンド

config rogue adhoc

show rogue adhoc summary

show rogue client summary

show rogue ignore-list

show rogue rule summary

config rogue ap valid-client

アラームだけを生成する、または信頼できるクライアントが関連付けられている不正なアクセス ポイントを自動的に阻止するには、**config rogue ap valid-client** コマンドを使用します。

config rogue ap valid-client {**alarm** | **auto-contain**}

構文の説明

alarm	不正なアクセス ポイントが有効なクライアントに関連付けられていることが検出されると、アラームだけが生成されます。
auto-contain	信頼できるクライアントに関連付けられている不正なアクセス ポイントを自動的に阻止します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

いずれかの containment コマンドを入力すると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療（ISM）帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、有効なクライアントに関連付けられている不正なアクセス ポイントを自動的に阻止する例を示します。

```
(Cisco Controller) > config rogue ap valid-client auto-contain
```

関連コマンド

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue client

不正なクライアントを設定するには、**config rogue client** コマンドを使用します。

config rogue client {**aaa** {**enable** | **disable**} | **alert** *ap_mac* | **contain** *client_mac* | **delete** {**state** {**alert** | **any** | **contained** | **contained-pending**} | **all** | **mac-address** *client_mac*} | **mse**{**enable** | **disable**} } }

構文の説明

aaa	不正なクライアントが有効なクライアントかどうかを検証するように AAA サーバまたはローカル データベースを設定します。デフォルトではディセーブルになっています。
enable	AAA サーバまたはローカルデータベースを有効にして、不正なクライアント MAC アドレスが有効かどうかを確認します。
disable	AAA サーバまたはローカルデータベースを無効にして、不正なクライアント MAC アドレスが有効かどうかを確認しないようにします。
alert	システム管理者に即座にアラートを発信し、必要な措置を促すようにコントローラを設定します。
ap_mac	アクセス ポイントの MAC アドレス。
contain	危険性のあるデバイスを阻止して、そのデバイスの信号が認証されたクライアントに干渉しないようにコントローラを設定します。
client_mac	不正なクライアントの MAC アドレス。
delete	不正なクライアントを削除します。
state	不正なクライアントをその状態に応じて削除します。
alert	アラート状態の不正クライアントを削除します。
any	任意の状態の不正クライアントを削除します。
contained	阻止状態になっているすべての不正クライアントを削除します。
contained-pending	阻止保留中の状態のすべての不正クライアントを削除します。

all	すべての不正クライアントを削除します。
mac-address	設定済みMACアドレスを持つ不正クライアントを削除します。
mse	不正クライアントが有効なクライアントかどうかをMSEを使用して検証します。デフォルトではディセーブルになっています。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

MSE と AAA に対して同時に不正クライアントを検証することはできません。

次に、AAA サーバまたはローカル データベースが MAC アドレスを確認できるようにする例を示します。

```
(Cisco Controller) > config rogue client aaa enable
```

次に、AAA サーバまたはローカル データベースが MAC アドレスを確認できないようにする例を示します。

```
(Cisco Controller) > config rogue client aaa disable
```

関連コマンド

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue containment

不正な阻止を設定するには、**config rogue containment** コマンドを使用します。

config rogue containment {**flexconnect** | **auto-rate**} {**enable** | **disable**}

構文の説明

flexconnect	スタンドアロンFlexConnect APの不正な阻止を設定します。
auto-rate	不正な阻止の自動レート選択を設定します。
enable	不正な阻止を有効にします。
disable	不正な阻止を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

次のテーブルに、不正な阻止の自動レート選択の詳細を示します。

表 *8:* 不正な阻止の自動レート選択

RSSI (dBm)	802.11b/g Tx レート（Mbps）	802.11a Tx レート（Mbps）
–74	1	6
–70	2	12
-55	5.5	12
< – 40	5.5	18

次に、不正な阻止の自動レート選択を有効にする例を示します。

```
(Cisco Controller) > config rogue containment auto-rate enable
```

config rogue detection

不正の検出を有効または無効にするには、**config rogue detection** コマンドを使用します。

（注） AP 自体が **all** キーワードで設定されている場合、**all access points** の場合は **all** というキーワードを持つ AP に優先します。

config rogue detection {**enable** | **disable**} {*cisco_ap* | **all**}

構文の説明

enable	このアクセス ポイントにおける不正の検出を有効にします。
disable	このアクセス ポイントにおける不正の検出を無効にします。
cisco_ap	シスコ アクセス ポイント。
all	すべてのアクセス ポイントを指定します。

コマンド デフォルト

デフォルトの不正の検出値が有効になります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

OfficeExtend アクセス ポイントを除き、コントローラに接続されたすべてのアクセス ポイントに対し、不正の検出がデフォルトで有効にされます。OfficeExtend アクセス ポイントは室内環境に導入され、多くの場合、大量の不正なデバイスを検出します。

次に、アクセス ポイント Cisco_AP の不正の検出を有効にする例を示します。

```
(Cisco Controller) > config rogue detection enable Cisco_AP
```

関連コマンド

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection client-threshold

アクセス ポイントの不正なクライアントしきい値を設定するには、**config rogue detection client-threshold** コマンドを使用します。

config rogue detection client-threshold *value*

構文の説明

value	アクセス ポイントでの不正なクライアント数のしきい値。この値を超えると Cisco Wireless LAN Controller（WLC）からトラップが送信されます。有効な範囲は 1 ～ 256 です。この機能を無効にするには 0 を入力します。

コマンド デフォルト

デフォルトの不正クライアントのしきい値は 12 です。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

次に、不正クライアントのしきい値を設定する例を示します。

```
(Cisco Controller) >config rogue detection client-threshold 200
```

config rogue detection min-rssi

AP が不正を検出し、コントローラで不正なエントリを作成できる受信信号強度インジケータ（RSSI）の最小値を設定するには、**config rogue detection min-rssi** コマンドを使用します。

config rogue detection min-rssi *rssi-in-dBm*

構文の説明

rssi-in-dBm	RSSI の最小値。有効な範囲は –70 ～ –128 dBm で、デフォルト値は –128 dBm です。

コマンド デフォルト

AP の不正を検出するデフォルトの RSSI 値は、-128 dBm です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この機能は、すべての AP モードに適用できます。

RSSI 値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、AP が不正を検出する最小 RSSI 値を指定することで、このオプションを使用して不正をフィルタリングすることができます。

次に、RSSI の最小値を設定する例を示します。

```
(Cisco Controller) > config rogue detection min-rssi -80
```

関連コマンド

config rogue detection

show rogue ap clients

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection monitor-ap

すべての監視モードの Cisco AP に対する不正レポートの間隔を設定するには、**config rogue detection monitor-ap** コマンドを使用します。

config rogue detection monitor-ap {**report-interval** | **transient-rogue-interval**} *time-in-seconds*

構文の説明

report-interval	不正レポートが送信される間隔を指定します。
transient-rogue-interval	最初に不正に対するスキャンを実行した後に、定期的にスキャンを行う間隔を指定します。
time-in-seconds	秒単位の時間。有効な範囲は次のとおりです。 • 10 ~ 300： **report-interval** • 120 ~ 1800： **transient-rogue-interval**

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

この機能は、モニタ モードの AP のみに適用されます。

一時的な間隔値を使用して、APが不正をスキャンする間隔を制御できます。APでは、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。

この機能には次の利点があります。

- AP からコントローラへの不正 AP レポートが短くなる。
- 一時的不正エントリをコントローラで回避できる。
- 一時的不正への不要なメモリ割り当てを回避できる。

次に、不正レポートの間隔を 60 秒に設定する例を示します。

```
(Cisco Controller) > config rogue detection monitor-ap report-interval 60
```

次に、一時的不正の間隔を 300 秒に設定する例を示します。

```
(Cisco Controller) > config rogue detection monitor-ap transient-rogue-interval 300
```

関連コマンド

config rogue detection

config rogue detection min-rssi

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection report-interval

不正検出レポート間隔を設定するには、**config rogue detection report-interval** コマンドを使用します。

config rogue detection report-interval *time*

構文の説明

time	アクセス ポイントからコントローラに不正検出レポートを送信する間隔（秒単位）です。範囲は 10 ～ 300 です。

コマンド デフォルト

デフォルトの不正検出レポート間隔は 10 秒です。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

この機能は、監視モードのアクセス ポイントのみに適用されます。

次に、不正検出レポート間隔を設定する例を示します。

```
(Cisco Controller) >config rogue detection report-interval 60
```

config rogue detection security-level

不正検出セキュリティ レベルを設定するには、**config rogue detection security-level** コマンドを使用します。

config rogue detection security-level {**critical** | **custom** | **high** | **low**}

構文の説明

critical	不正検出セキュリティ レベルを「重大」に設定します。
custom	不正検出セキュリティ レベルを「カスタム」に設定し、不正なポリシーパラメータを設定できるようになります。
high	不正検出セキュリティ レベルを「高」に設定します。このセキュリティ レベルは、中規模またはあまり重大でない展開のための基本的な不正検出と自動阻止を設定します。このセキュリティ レベルではRogue Location Discovery Protocol（RLDP）は無効です。
low	不正検出セキュリティ レベルを「低」に設定します。このセキュリティ レベルは、小規模の展開のための基本的な不正検出を設定します。このセキュリティ レベルでは自動阻止はサポートされていません。

コマンド デフォルト

デフォルトの不正検出セキュリティ レベルは「カスタム」です。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

次に、不正検出セキュリティ レベルを「高」に設定する例を示します。

```
(Cisco Controller) > config rogue detection security-level high
```

config rogue detection transient-rogue-interval

不正検出の一時的間隔を設定するには、**config rogue detection transient-rogue-interval** コマンドを使用します。

config rogue detection transient-rogue-interval *time*

構文の説明

time	最初に不正がスキャンされた後、アクセス ポイントが継続的に不正をスキャンする必要のある間隔（秒単位）です。有効な範囲は 120 ～ 1800 です。

コマンド デフォルト

各セキュリティ レベルのデフォルトの不正検出の一時的間隔は次のとおりです。

- 低：120 秒
- 高：300 秒
- 重大：600 秒

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

この機能は、監視モードのアクセス ポイントのみに適用されます。

連続的に不正がスキャンされると、更新情報が定期的に Cisco Wireless LAN Controller（WLC）へ送信されます。アクセス ポイントは、非常に短い時間だけアクティブな一時的不正をフィルタリングし、その後は活動を停止します。

次に、不正検出の一時的間隔を設定する例を示します。

```
(Cisco Controller) > config rogue detection transient-rogue-interval 200
```

config rogue rule

不正分類ルールを追加および設定するには、**config rogue rule** コマンドを使用します。

config rogue rule {**add ap priority** *priority* **classify** {**custom** *severity-score classification-name* | **friendly** | **malicious**} **notify** {**all** | **global** | **none** | **local**} **state** {**alert** | **contain** | **delete** | **internal** | **external**} *rule_name* | **classify** {**custom** *severity-score classification-name* | **friendly** | **malicious**} *rule_name* | **condition ap** {**set** | **delete**} *condition_type condition_value rule_name* | {**enable** | **delete** | **disable**} {**all** | *rule_name*} | **match** {**all** | **any**} | **priority** *priority* | **notify** {**all** | **global** | **none** | **local**} *rule_name* | **state** {**alert** | **contain** | **internal** | **external**} *rule_name*}

構文の説明

add ap priority	指定した基準および優先順位に一致するルールを追加します。
priority	このルールのルール リスト内での優先順位。
classify	ルールの分類を指定します。
custom	カスタムとしてのルールに一致するデバイスを分類します。
severity-score	ルールのカスタム分類の重大度スコア。範囲は 1 ～ 100 です。
classification-name	カスタム分類の名前。名前は最大 32 文字の英数字で、大文字と小文字を区別します。
friendly	ルールを危険性のないルールとして分類します。
malicious	ルールを悪意のあるルールとして分類します。
notify	ルールの照合における通知のタイプを設定します。
all	コントローラ、および Cisco Prime Infrastructure などのトラップ レシーバに通知します。
global	Cisco Prime Infrastructure などのトラップ レシーバだけに通知します。
local	コントローラだけに通知します。
none	コントローラ、および Cisco Prime Infrastructure などのトラップ レシーバのどちらにも通知しません。

state	ルールの照合後の不正なアクセス ポイントの状態を設定します。
alert	ネイバー リストにない、またはユーザが設定した危険性のないMACのリストに記載されていない不正アクセス ポイントのアラート状態を設定します。コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。
contain	不正アクセス ポイントをcontainの状態に設定します。コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
delete	不正アクセス ポイントを delete の状態に設定します。
external	ネットワークの外側にあり、WLAN のセキュリティに脅威を与えない不正アクセス ポイントの外部状態を設定します。コントローラはこの不正なアクセス ポイントの存在を認識しています。
internal	ネットワークの内側にあり、WLAN のセキュリティに脅威を与えない不正アクセス ポイントのアラート状態を設定します。コントローラはこの不正なアクセス ポイントを信頼します。
rule_name	コマンドを適用するルールまたは新しいルールの名前。
condition ap	不正なアクセス ポイントが満たす必要のあるルールに条件を指定します。
set	不正なアクセス ポイントが満たす必要のあるルールに条件を追加します。
delete	不正なアクセス ポイントが満たす必要のあるルールの条件を削除します。

condition_type	設定する条件のタイプ。条件タイプは以下のとおりです。 • client-count：最小数のクライアントが不正なアクセス ポイントにアソシエートされていることが条件となります。有効な範囲は 1 ～ 10 です。 • duration：不正なアクセス ポイントが最短期間で検出されることが条件となります。有効な範囲は 0 ～ 3600 秒です。 • managed-ssid：不正なアクセス ポイントの SSID がコントローラで認識される必要があります。 • no-encryption：不正なアクセス ポイントのアドバタイズされた WLAN で暗号化が無効になっている必要があります。 • rssi：不正なアクセス ポイントには、最小の RSSI 値が必要です。範囲は、–95 ～ -50 dBm です。 • ssid：不正なアクセス ポイントには、特定の SSID が必要です。 • substring-ssid：不正なアクセス ポイントにユーザ設定 SSID のサブストリングが存在する必要があります。
condition_value	条件の値。この値は、condition_type によって異なります。たとえば、条件タイプが ssid の場合、条件値は SSID 名か all です。
enable	すべてのルールまたは特定のルール 1 つを有効にします。
delete	すべてのルールまたは特定のルール 1 つを削除します。
disable	すべてのルールまたは特定のルール 1 つを削除します。

match	検出された不正なアクセス ポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるためには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。
all	定義されているすべてのルールを指定します。
any	特定の条件を満たしているルールを指定します。
priority	特定のルールの優先順位を変更し、それに応じて、リスト内のその他のルールの優先順位を調整します。

コマンド デフォルト

不正ルールが設定されていません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

変更内容を有効にするには、ルールを有効にする必要があります。最大 64 のルールを設定できます。

不正なルールの RSSI 基準に応じた不正な AP の再分類は、RSSI が設定された RSSI 値から +/- 2 dBm を超えて変更された場合のみ発生します。手動および自動による分類は、カスタムの不正なルールよりも優先されます。クラス タイプが未分類に変更され、状態が alert に変更されると、ルールは手動で変更された不正に適用されます。アドホックの不正は分類され、保留状態にはなりません。最大 50 個の分類タイプを設定できます。

次に、優先順位が 1、分類が friendly である、rule_1 という名前のルールを作成する例を示します。

```
(Cisco Controller) > config rogue rule add ap priority 1 classify friendly rule_1
```

次に、rule_1 を有効にする例を示します。

```
(Cisco Controller) > config rogue rule enable rule_1
```

次に、最後のコマンドの優先順位を変更する例を示します。

```
(Cisco Controller) > config rogue rule priority 2 rule_1
```

次に、最後のコマンドの分類を変更する例を示します。

```
(Cisco Controller) > config rogue rule classify malicious rule_1
```

次に、最後のコマンドを無効にする例を示します。

```
(Cisco Controller) > config rogue rule disable rule_1
```

次に、rule-5 のユーザが設定した SSID リストから SSID_2 を削除する例を示します。

```
(Cisco Controller) > config rogue rule condition ap delete ssid ssid_2 rule-5
```

次に、カスタムの不正なルールを作成する例を示します。

```
(Cisco Controller) > config rogue rule classify custom 1 VeryMalicious rule6
```

config rogue rule condition ap

不正アクセス ポイントの不正ルールの条件を設定するには、**config rogue rule condition ap** コマンドを使用します。

config rogue rule condition ap {**set** {**client-count** *count* | **duration** *time* | **managed-ssid** | **no-encryption** | **rssi** *rssi* | **ssid** *ssid* | **substring-ssid** *substring-ssid*} | **delete** {**all** | **client-count** | **duration** | **managed-ssid** | **no-encryption** | **rssi** | **ssid** | **substring-ssid**} *rule_name*

構文の説明

set	不正なアクセス ポイントが満たす必要のあるルールに条件を設定します。
client-count	不正アクセス ポイントに最小数のクライアントをアソシエートできるようにします。
count	不正アクセス ポイントにアソシエートする最小数のクライアント。範囲は 1 ～ 10 です。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。
duration	不正アクセス ポイントを最小期間で検出できるようにします。
time	不正アクセス ポイントを検出する最小期間（秒単位）。範囲は 0 ～ 3600 です。
managed-ssid	不正アクセス ポイントの SSID がコントローラで認識されるようにします。
no-encryption	不正アクセス ポイントのアドバタイズされた WLAN で暗号化を無効にできるようにします。不正なアクセス ポイントの暗号化が無効になっている場合、より多くのクライアントがそのアクセス ポイントに対してアソシエートを試行します。
rssi	不正なアクセス ポイントが最小の受信信号強度インジケータ（RSSI）値を持てるようにします。
rssi	アクセス ポイントに必要な最小 RSSI 値（dBm）。範囲は、–95 ～ -50 です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。
ssid	不正なアクセス ポイントが特定の SSID を持てるようにします。
ssid	不正アクセス ポイントの SSID。
substring-ssid	不正アクセス ポイントがユーザ設定の SSID のサブストリングを持てるようにします。
substring-ssid	ユーザ設定 SSID のサブストリング。たとえば、ABCDE という SSID がある場合、ABCD または ABC としてサブストリングを指定できます。パターンが一致する複数の SSID を分類することができます。

delete	不正なアクセス ポイントが満たす必要のあるルールの条件を削除します。
all	すべての不正ルールの条件を削除します。
rule_name	コマンドが適用される不正ルール。

コマンド デフォルト

RSSI のデフォルト値は 0 dBm です。

デフォルトの間隔値は 0 秒です。

クライアント数のデフォルト値は 0 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

不正ルールあたり最大 25 の SSID を設定することができます。不正ルールあたり最大 25 の SSID サブストリングを設定することができます。

次に、RSSI 不正ルールの条件を設定する例を示します。

```
(Cisco Controller) > config rogue rule condition ap set rssi -50
```

config remote-lan session-timeout

クライアント セッションのタイムアウトを設定するには、**config remote-lan session-timeout** コマンドを使用します。

config remote-lan session-timeout *remote-lan-id seconds*

構文の説明

remote-lan-id	リモート LAN の識別子。有効な値は、1 ～ 512 です。
seconds	タイムアウトまたはセッション時間（秒）。値 0 は、タイムアウトなしに相当します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ID 1 のリモート LAN で、クライアント セッション タイムアウトを 6000 秒に設定する例を示します。

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

config rfid auto-timeout

無線周波数ID（RFID）タグの自動タイムアウトを設定するには、**config rfid auto-timeout** コマンドを使用します。

config rfid auto-timeout {**enable** | **disable**}

構文の説明

enable	自動タイムアウトをイネーブルにします。
disable	自動タイムアウトをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、RFID タグの自動タイムアウトをイネーブルにする例を示します。

```
(Cisco Controller) > config rfid auto-timeout enable
```

関連コマンド

show rfid summary

config rfid status

config rfid timeout

config rfid status

無線周波数 ID（RFID）タグのデータ追跡を設定するには、**config rfid status** コマンドを使用します。

config rfid status {**enable** | **disable**}

構文の説明

enable	RFID タグ追跡をイネーブルにします。
disable	RFID タグ追跡をイネーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RFID タグ追跡を設定する例を示します。

```
(Cisco Controller) > config rfid status enable
```

関連コマンド

show rfid summary

config rfid auto-timeout

config rfid timeout

config rfid timeout

スタティック無線周波数 ID（RFID）タグのデータ タイムアウトを設定するには、**config rfid timeout** コマンドを使用します。

config rfid timeout *seconds*

構文の説明

seconds	秒単位でのタイムアウト（60 ～ 7,200）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、スタティック RFID タグのデータ タイムアウトを 60 秒に設定する例を示します。

```
(Cisco Controller) > config rfid timeout 60
```

関連コマンド

show rfid summary

config rfid statistics

config rogue ap timeout

不正なアクセスポイントおよびクライアントのエントリが期限切れとなり、リストから削除されるまでの秒数を指定するには、**config rogue ap timeout** コマンドを使用します。

config rogue ap timeout *seconds*

構文の説明

seconds	240 ～ 3600 秒までの値。デフォルト値は 1200 秒です。

コマンド デフォルト

不正なアクセスポイントおよびクライアントのエントリが期限切れとなるまでのデフォルトの秒数は、1200 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、不正アクセス ポイントとクライアント リストのエントリの有効期限を 2400 秒に設定する例を示します。

```
(Cisco Controller) > config rogue ap timeout 2400
```

関連コマンド

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config route add

サービス ポートから専用ワークステーションの IP アドレス範囲へのネットワーク ルートを設定するには、**config route add** コマンドを使用します。

config route add *ip_address netmask gateway*

構文の説明

ip_address	ネットワーク IP アドレス。
netmask	ネットワークのサブネット マスク。
gateway	ルート ネットワークのゲートウェイの IP アドレス。

コマンド デフォルト

なし

使用上のガイドライン

IP_address は IPv4 アドレスのみをサポートします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。 このコマンドは、IPv4 アドレス形式のみをサポートします。

次に、専用ワーク ステーションの IP アドレス 10.1.1.0、サブネット マスク 255.255.255.0、およびゲートウェイ 10.1.1.1 へのネットワーク ルートを設定する例を示します。

```
(Cisco Controller) > config route add 10.1.1.0 255.255.255.0 10.1.1.1
```

config route delete

サービス ポートからネットワーク ルートを削除するには、**config route delete** コマンドを使用します。

config route delete *ip_address*

構文の説明

ip_address	ネットワーク IP アドレス。

コマンド デフォルト

なし

使用上のガイドライン

IP_address は IPv4 アドレスのみをサポートします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv6 アドレス形式のみをサポートします。

次に、ネットワーク IP アドレス 10.1.1.0 からルートを削除する例を示します。

```
(Cisco Controller) > config route delete 10.1.1.0
```

config serial baudrate

シリアル ポートのボー レートを設定するには、**config serial baudrate** コマンドを使用します。

config serial baudrate {**1200** | **2400** | **4800** | **9600** | **19200** | **38400** | **57600**}

構文の説明

1200	サポートされている接続速度を 1200 に指定します。
2400	サポートされている接続速度を 2400 に指定します。
4800	サポートされている接続速度を 4800 に指定します。
9600	サポートされている接続速度を 9600 に指定します。
19200	サポートされている接続速度を 19200 に指定します。
38400	サポートされている接続速度を 38400 に指定します。
57600	サポートされている接続速度を 57600 に指定します。

コマンド デフォルト

デフォルトのシリアル ポートのボー レートは 9600 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、9600 のデフォルトの接続速度でシリアル ボー レートを設定する例を示します。

```
(Cisco Controller) > config serial baudrate 9600
```

config serial timeout

シリアル ポート セッションのタイムアウトを設定するには、**config serial timeout** コマンドを使用します。

config serial timeout *minutes*

構文の説明

minutes	分単位でのタイムアウト（0 ～ 160 分）。値 0 は、タイムアウトなしを示します。

コマンド デフォルト

0（タイムアウトなし）

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用して、Cisco ワイヤレス LAN コントローラ前面のシリアル接続のタイムアウトを 0 ～ 160 分の範囲で設定します（0 はタイムアウトなし）。

次に、シリアル ポート セッションのタイムアウトを 10 分に設定する例を示します。

```
(Cisco Controller) > config serial timeout 10
```

config service timestamps

メッセージ ログのタイムスタンプを有効または無効にするには、**config service timestamps** コマンドを使用します。

config service timestamps {**debug** | **log**} {**datetime** | **disable**}

構文の説明

debug	デバッグ メッセージのタイムスタンプを設定します。
log	ログ メッセージのタイムスタンプを設定します。
datetime	標準日付を使用して、タイムスタンプ メッセージ ログを指定します。
disable	メッセージ ログにタイムスタンプが設定されないように指定します。

コマンド デフォルト

デフォルトでは、メッセージ ログのタイムスタンプは無効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、標準日付を使用して、タイムスタンプ メッセージ ログを設定する例を示します。

```
(Cisco Controller) > config service timestamps log datetime
```

次に、メッセージ ログにタイムスタンプが設定されないようにする例を示します。

```
(Cisco Controller) > config service timestamps debug disable
```

関連コマンド

show logging

config sessions maxsessions

Cisco Wireless LAN Controller で許可する Telnet CLI セッション数を設定するには、**config sessions maxsessions** コマンドを使用します。

config sessions maxsessions *session_num*

構文の説明

session_num	0 ～ 5 のセッション数。

コマンド デフォルト

Cisco WLC で許可される Telnet CLI セッションのデフォルト数は 5 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

最大 5 セッションが許可されます。0 に設定するとすべての Telnet CLI セッションが禁止されます。

次に、許可される CLI セッションの数を 2 に設定する例を示します。

```
(Cisco Controller) > config sessions maxsessions 2
```

関連コマンド

show sessions

config sessions timeout

Telnet CLI セッションの無活動タイムアウトを設定するには、**config sessions timeout** コマンドを使用します。

config sessions timeout *timeout*

構文の説明

timeout	分単位の Telnet セッションのタイムアウト（0 ～ 160 分）。値 0 は、タイムアウトなしを示します。

コマンド デフォルト

Telnet CSI セッションのデフォルトの無活動タイムアウトは 5 分です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Telnet セッションの無活動タイムアウトを 20 分に設定する例を示します。

```
(Cisco Controller) > config sessions timeout 20
```

関連コマンド

show sessions

config slot

さまざまなスロット パラメータを設定するには、**config slot** コマンドを使用します。

config slot *slot_id* {**enable** | **disable** | **channel ap** | **chan_width** | **txpower ap** | **antenna extAntGain** *antenna_gain* | **rts**} *cisco_ap*

構文の説明

slot_id	チャネルが割り当てられたスロットのダウンリンク無線。リリース 7.5 以降のリリースでは、スロット 1 で 802.11a、スロット 2 で 802.11ac を設定できます。
enable	スロットを有効にします。
disable	スロットを無効にします。
channel	スロットにチャネルを設定します。
ap	1 個の 802.11a Cisco アクセス ポイントを設定します。
chan_width	スロットのチャネル幅を設定します。
txpower	スロットの Tx 電力を設定します。
antenna	802.11a アンテナを設定します。
extAntGain	802.11a 外部アンテナ ゲインを設定します。
antenna_gain	0.5 dBi 単位の外部アンテナ ゲイン値（例：2.5 dBi = 5）。
rts	アクセス ポイントに対して RTS/CTS を設定します。
cisco_ap	チャネルが設定されている Cisco アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイント abc のスロット 3 を有効にする例を示します。

```
(Cisco Controller) >config slot 3 enable abc
```

次に、アクセス ポイント abc の RTS を設定する例を示します。

```
(Cisco Controller) >config slot 2 rts abc
```

config switchconfig boot-break

システムの起動時にEscキーを押して、ブートプロンプトに割り込む操作をイネーブルまたはディセーブルにするには、**config switchconfig boot-break** コマンドを使用します。

config switchconfig boot-break {**enable** | **disable**}

構文の説明

enable	システムの起動時に Esc キーを押して、ブート プロンプトに割り込む操作をイネーブルにします。
disable	システムの起動時に Esc キーを押して、ブート プロンプトに割り込むことをディセーブルにします。

コマンド デフォルト

デフォルトでは、システムの起動時にEscキーを押して、ブートプロンプトに割り込む操作は無効です。

使用上のガイドライン

ブートにプロンプトへの割り込みをイネーブルまたはディセーブルにする前に、連邦情報処理標準（FIPS）モードの前提条件である機能をイネーブルにする必要があります。

次に、システムの起動時に Esc キーを押して、ブート プロンプトに割り込む操作をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig boot-break enable
```

関連コマンド

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig strong-pwd

config switchconfig fips-prerequisite

連邦情報処理標準（FIPS）モードの前提条件である機能をイネーブルまたはディセーブルにするには、**config switchconfig fips-prerequisite** コマンドを使用します。

config switchconfig fips-prerequisite {**enable** | **disable**}

構文の説明

enable	FIPS モードの前提条件である機能をイネーブルにします。
disable	FIPS モードの前提条件である機能をディセーブルにします。

コマンド デフォルト

デフォルトでは、FIPS モードの前提条件である機能は無効です。

使用上のガイドライン

FIPS の前提条件である機能をイネーブルまたはディセーブルにするには、FIPS 承認のシークレットを設定する必要があります。

次に、FIPS モードの前提条件である機能をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig fips-prerequisite enable
```

関連コマンド

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig boot-break

config switchconfig strong-pwd

config switchconfig ucapl

コントローラの米国の国防総省（DoD）の統一機能承認製品リスト（APL）認証を設定するには、**config switchconfig wlancc** コマンドを使用します。

config switchconfig ucapl {**enable** | **disable**}

構文の説明

enable	コントローラで UCAPL を有効にします。
disable	コントローラで UCAPL を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、コントローラで UCAPL をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig ucapl enable
```

config switchconfig wlancc

コントローラでWLANコモンクライテリア（CC）を設定するには、**config switchconfig wlancc** コマンドを使用します。

config switchconfig wlancc {**enable** | **disable**}

構文の説明

enable	コントローラの WLAN CC を有効にします。
disable	コントローラの WLAN CC を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、コントローラで WLAN CC を有効にする例を示します。

```
(Cisco Controller) > config switchconfig wlancc enable
```

config switchconfig strong-pwd

新しく作成されたパスワードの強度に対するコントローラのチェックをイネーブルまたはディセーブルにするには、**config switchconfig strong-pwd** コマンドを使用します。

config switchconfig strong-pwd {**case-check** | **consecutive-check** | **default-check** | **username-check** | **position-check** | **case-digit-check** | **minimum** {**upper-case** | **lower-case** | **digits** | **special-chars**} *no._of_characters* | **min-length** | *password_length* | **lockout**{**mgmtuser** | **snmpv3user** | **time** | **attempts**} | **lifetime** {**mgmtuser** | **snmpv3user**} *lifetime* | **all-checks**} {**enable** | **disable**}

構文の説明

case-check	小文字、大文字、数字、または特種文字から少なくとも 3 つが組み合わされているかをチェックします。
consecutive-check	同じ文字が 3 回使用されていないかをチェックします。
default-check	デフォルト値またはそれらのバリアントが使用されていないかをチェックします。
username-check	ユーザ名が指定されているかどうかをチェックします。
position-check	古いパスワードからの変更が 4 文字あるかどうかをチェックします。
case-digit-check	パスワードに大文字、小文字、数字、特殊文字の 4 つすべての組み合わせが含まれているかどうかをチェックします
minimum	パスワードに大文字と小文字、数字、特殊文字の最小数が含まれているかどうかをチェックします。
upper-case	パスワードに大文字の最小数が含まれているかどうかをチェックします。
lower-case	パスワードに小文字の最小数が含まれているかどうかをチェックします。
digits	パスワードに数字の最小数が含まれているかどうかをチェックします。
special-chars	パスワードに特殊文字の最小数が含まれているかどうかをチェックします。
min-length	パスワードの最小文字数を設定します。

password_length	パスワードの最小文字数。値の範囲は 3 ～ 24 文字です（大文字と小文字を区別します）。
lockout	管理ユーザまたは Simple Network Management Protocol version 3（SNMPv33）ユーザのロックアウト機能を設定します。
mgmtuser	連続試行失敗回数が管理ユーザのロックアウト試行回数を超えると、管理ユーザをロックします。
snmpv3user	連続試行失敗回数が SNMPv3 ユーザのロックアウト試行回数を超えると、SNMPv3 ユーザをロックします。
time	管理ユーザまたは SNMPv3 ユーザがロックされているときの、ロックアウト試行後の継続時間を設定します。
attempts	不正パスワードの連続入力回数を設定します。この回数を超えると管理ユーザまたはSNMPv3 ユーザがロックされます。
lifetime	パスワードのエイジングが原因で、管理ユーザまたは SNMPv3 ユーザによるパスワードの変更が必要になるまでの日数を設定します。
mgmtuser	パスワードのエイジングが原因で、管理ユーザによるパスワードの変更が必要になるまでの日数を設定します。
snmpv3user	パスワードのエイジングが原因で、SNMPv3 ユーザによるパスワードの変更が必要になるまでの日数を設定します。
lifetime	パスワードのエイジングが原因で、管理ユーザまたは SNMPv3 ユーザによるパスワードの変更が必要になるまでの日数。*lifetime*
all-checks	すべてのケースをチェックします。
enable	アクセス ポイントおよび Cisco WLC の強力なパスワード チェックを有効にします。
disable	アクセス ポイントおよび Cisco WLC の強力なパスワード チェックを無効にします。

コマンド デフォルト なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、強力なパスワード チェック機能をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig strong-pwd case-check enable
```

関連コマンド

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig boot-break

config switchconfig flowcontrol

802.3x のフロー制御を有効または無効にするには、**config switchconfig flowcontrol** コマンドを使用します。

config switchconfig flowcontrol {**enable** | **disable**}

構文の説明

enable	802.3x フロー制御をイネーブルにします。
disable	802.3x フロー制御をディセーブルにします。

コマンド デフォルト

デフォルトでは、802.3X のフロー制御は無効にされています。

次に、Cisco ワイヤレス LAN コントローラ パラメータで 802.3x フロー制御をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig flowcontrol enable
```

関連コマンド

show switchconfig

config switchconfig mode

レイヤ 2 またはレイヤ 3 の Lightweight Access Port Protocol（LWAPP）トランスポート モードを設定するには、**config switchconfig mode** コマンドを使用します。

config switchconfig mode {**L2** | **L3**}

構文の説明

L2	トランスポート モードとしてレイヤ 2 を指定します。
L3	トランスポート モードとしてレイヤ 3 を指定します。

コマンド デフォルト

デフォルトのトランス ポート モードは L3 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LWAPP トランスポート モードをレイヤ 3 に設定する例を示します。

```
(Cisco Controller) > config switchconfig mode L3
```

関連コマンド

show switchconfig

config switchconfig secret-obfuscation

機密事項の難読化を有効または無効にするには、**config switchconfig secret-obfuscation** コマンドを使用します。

config switchconfig secret-obfuscation {**enable** | **disable**}

構文の説明

enable	機密事項の難読化をイネーブルにします。
disable	機密事項の難読化をディセーブルにします。

コマンド デフォルト

機密事項およびユーザ パスワードは、エクスポートされた XML 設定ファイルでは難読化されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

設定ファイルの機密の内容を安全に保護するには、機密事項の難読化を無効にしないでください。設定ファイルのセキュリティをさらに強化するには、設定ファイルの暗号化を有効にします。

次に、機密事項の難読化をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig secret-obfuscation enable
```

関連コマンド

show switchconfig

config sysname

Cisco Wireless LAN Controller のシステム名を設定するには、**config sysname** コマンドを使用します。

config sysname *name*

構文の説明

name	システム名。名前には、最大31文字の英数字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、Ent_01 という名前のシステムを設定する例を示します。

```
(Cisco Controller) > config sysname Ent_01
```

関連コマンド

show sysinfo

config snmp community accessmode

SNMP コミュニティのアクセス モード（読み取り専用または読み取りと書き込み）を変更するには、**config snmp community accessmode** コマンドを使用します。

config snmp community accessmode {**ro** | **rw**} *name*

構文の説明

ro	読み取り専用モードを指定します。
rw	読み取り/書き込みモードを指定します。
name	SNMP コミュニティ名。

コマンド デフォルト

デフォルトでは、次の設定を持つ 2 つのコミュニティが設定されています。

```
SNMP Community Name Client IP Address Client IP Mask   Access Mode Status
------------------- ----------------- ---------------- ----------- ------
public              0.0.0.0           0.0.0.0          Read Only   Enable
private             0.0.0.0           0.0.0.0          Read/Write  Enable
```

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、SNMP コミュニティに読み取り/書き込みアクセス モードを設定する例を示します。

```
(Cisco Controller) > config snmp community accessmode rw private
```

関連コマンド

show snmp community

config snmp community mode

config snmp community create

config snmp community delete

config snmp community ipaddr

config snmp community create

新規 SNMP コミュニティを作成するには、**config snmp community create** コマンドを使用します。

config snmp community create *name*

構文の説明

name	最大 16 文字の SNMP コミュニティ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

次のコマンドを使用して、デフォルト設定の新規コミュニティを作成します。

次に、test という名前の新しい SNMP コミュニティを作成する例を示します。

```
(Cisco Controller) > config snmp community create test
```

関連コマンド

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community delete

config snmp community ipaddr

config snmp community delete

SNMP コミュニティを削除するには、**config snmp community delete** コマンドを使用します。

config snmp community delete *name*

構文の説明

name	SNMP コミュニティ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、test という名前の SNMP コミュニティを削除する例を示します。

```
(Cisco Controller) > config snmp community delete test
```

関連コマンド

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community create

config snmp community ipaddr

config snmp community ipaddr

SNMP コミュニティの IPv4 または IPv6 アドレスを設定するには、**config snmp community ipaddr** コマンドを使用します。

config snmp community ipaddr *IP addr IPv4 mask/IPv6 Prefix lengthname*

構文の説明

ip-addr	SNMP コミュニティの IPv4 または IPv6 アドレス。
IPv4 mask/IPv6 Prefix length	SNMP コミュニティ IP マスク（IPv4 マスクまたは IPv6 プレフィックス長）。IPv6 プレフィックス長は、0 ～ 128 です。
name	SNMP コミュニティ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

- このコマンドは、IPv4 と IPv6 の両方のアドレスに適用されます。
- このコマンドは、デフォルトの SNMP コミュニティ（パブリック、プライベート）には適用されません。

次に、IPv4 アドレス 10.10.10.10、IPv4 マスク 255.255.255.0、および SNMP コミュニティ名 comaccess の SNMP コミュニティを設定する例を示します。

```
(Cisco Controller) > config snmp community ipaddr 10.10.10.10 255.255.255.0 comaccess
```

次に、IPv6 アドレス 2001:9:2:16::1、IPv6 プレフィックス長 60、および SNMP コミュニティ名 comaccess の SNMP コミュニティを設定する例を示します。

```
(Cisco Controller) > config snmp community ipaddr 2001:9:2:16::1 64 comaccess
```

config snmp community mode

SNMP コミュニティを有効または無効にするには、**config snmp community mode** コマンドを使用します。

config snmp community mode {**enable** | **disable**} *name*

構文の説明

enable	コミュニティをイネーブルにします。
disable	コミュニティをディセーブルにします。
name	SNMP コミュニティ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、public という名前の SNMP コミュニティを有効にする例を示します。

```
(Cisco Controller) > config snmp community mode disable public
```

関連コマンド

show snmp community

config snmp community delete

config snmp community accessmode

config snmp community create

config snmp community ipaddr

config snmp engineID

SNMP エンジン ID を設定するには、**config snmp engineID** コマンドを使用します。

config snmp engineID {*engine_id* | **default**}

構文の説明

engine_id	16 進数文字のエンジン ID（最小で 10 文字、最大で 24 文字を使用できます）。
default	デフォルトのエンジンIDをリストアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

SNMPエンジンIDは、管理用にデバイスを識別するために使用する一意の文字列です。デフォルトの文字列はシスコの番号とデバイスの最初のインターフェイスの MAC アドレスを使用して自動的に生成されるため、デバイスのエンジン ID を指定する必要があります。

エンジン ID を変更する場合、変更を有効にするにはリブートする必要があります。

注意 SNMP エンジン ID の値を変更すると、コマンド ラインに入力されたユーザのパスワードが MD5（Message Digest アルゴリズム 5）または SHA（セキュア ハッシュ アルゴリズム）セキュリティ ダイジェストに変換されます。このダイジェストはパスワードとローカル エンジン ID の両方に基づいています。コマンド ラインのパスワードは削除されます。このため、エンジン ID のローカル値を変更した場合は、SNMP ユーザのセキュリティ ダイジェストが無効となり、ユーザを再設定しなければなりません。

次に、値 fffffffffff を使用して SNMP エンジン ID を設定する例を示します。

```
(Cisco Controller) > config snmp engineID fffffffffff
```

関連コマンド

show snmpengineID

config snmp syscontact

SNMP システム接点名を設定するには、**config snmp syscontact** コマンドを使用します。

config snmp syscontact *contact*

構文の説明

contact	SNMP システム接点名。有効な値は、最大 255 文字の出力可能な文字です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、SNMP システム接点を Cisco WLAN Solution_administrator という名前に設定する例を示します。

```
(Cisco Controller) > config snmp syscontact Cisco WLAN Solution_administrator
```

config snmp syslocation

SNMP システムのロケーション名を設定するには、**config snmp syslocation** コマンドを使用します。

config snmp syslocation *location*

構文の説明

location	SNMP システムのロケーション名。有効な値は、最大 255 文字の出力可能な文字です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、SNMP システム ロケーション名を Building_2a に設定する例を示します。

```
(Cisco Controller) > config snmp syslocation Building_2a
```

config snmp trapreceiver create

サーバで SNMP トラップを受信するように設定するには、**config snmp trapreceiver create** コマンドを使用します。

config snmp trapreceiver create *name IP addr*

構文の説明

name	SNMP コミュニティ名。名前には、最大で 31 文字まで使用できます。
ip-addr	SNMP トラップを送信する場所の IPv4 または IPv6 アドレスを設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

このコマンドを実行して新しいサーバを追加するには、IPv4 または IPv6 アドレスが有効になっている必要があります。

次に、名前が test で IP アドレスが 10.1.1.1 の SNMP トラップ レシーバを持つ、新しい SNMP トラップ レシーバを追加する例を示します。

```
(Cisco Controller) > config snmp trapreceiver create test 10.1.1.1
```

次に、名前が test で IP アドレスが 2001:10:1:1::1 の SNMP トラップ レシーバを持つ、新しい SNMP トラップ レシーバを追加する例を示します。

```
(Cisco Controller) > config snmp trapreceiver create test 2001:10:1:1::1
```

config snmp trapreceiver delete

トラップ レシーバ リストからサーバを削除するには、**config snmp trapreceiver delete** コマンドを使用します。

config snmp trapreceiver delete *name*

構文の説明

name	SNMP コミュニティ名。名前は最大 16 文字で指定できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、test という名前のサーバを SNMP トラップ レシーバ リストから削除する例を示します。

```
(Cisco Controller) > config snmp trapreceiver delete test
```

関連コマンド

show snmp trap

config snmp trapreceiver mode

選択したサーバへのトラップの送信を有効または無効にするには、**config snmp trapreceiver mode** コマンドを使用します。

config snmp trapreceiver mode {**enable** | **disable**} *name*

構文の説明

enable	SNMP トラップをイネーブルにします。
disable	SNMP トラップ レシーバをディセーブルにします。
name	SNMP コミュニティ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用して、Cisco ワイヤレス LAN コントローラから選択したサーバへのトラップの送信をイネーブルまたはディセーブルにできます。

次に、SNMP トラップ レシーバが、server1 という名前のサーバにトラップを送信しないようにする例を示します。

```
(Cisco Controller) > config snmp trapreceiver mode disable server1
```

関連コマンド

show snmp trap

config snmp v3user create

バージョン 3 の SNMP ユーザを作成するには、**config snmp v3user create** コマンドを使用します。

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} [*auth_key*] [*encrypt_key*]

構文の説明

username	バージョン 3 の SNMP ユーザ名。
ro	読み取り専用ユーザ権限を指定します。
rw	読み取り/書き込みユーザ権限を指定します。
none	認証が必要ない場合に指定します。
hmacmd5	認証に Hashed Message Authentication コーディングのメッセージ ダイジェスト 5（HMAC-MD5）を指定します。
hmacsha	認証に Hashed Message Authentication コーディングのセキュア ハッシュ アルゴリズム（HMAC-SHA）を指定します。
none	暗号化が必要ない場合に指定します。
des	Cipher Block Chaining-Digital Encryption Standard（CBC-DES）暗号化を使用するように指定します。
aescfb128	Cipher Feedback Mode-Advanced Encryption Standard-128（CFB-AES-128）暗号化を使用するように指定します。
auth_key	（任意）HMAC-MD5 または HMAC-SHA 認証プロトコルの認証キー。
encrypt_key	（任意）CBC-DES または CFB-AES-128 暗号プロトコルの暗号キー。

コマンド デフォルト

SNMP v3 username AccessMode Authentication Encryption

```
------------------- ------------ -------------- -----------
default             Read/Write    HMAC-SHA       CFB-AES
```

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、読み取り専用権限を設定し、暗号化または認証を設定せずに、test という名前の SNMP ユーザ名を追加する例を示します。

```
(Cisco Controller) > config snmp v3user create test ro none none
```

関連コマンド

show snmpv3user

config snmp v3user delete

バージョン 3 の SNMP ユーザを削除するには、**config snmp v3user delete** コマンドを使用します。

config snmp v3user delete *username*

構文の説明

username	削除するユーザ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、test という名前の SNMP ユーザを削除する例を示します。

```
(Cisco Controller) > config snmp v3user delete test
```

関連コマンド

show snmp v3user

config snmp version

選択した SNMP バージョンを有効または無効にするには、**config snmp version** コマンドを使用します。

config snmp version {**v1** | **v2** | **v3**} {**enable** | **disable**}

構文の説明

v1	有効または無効にする SNMP バージョンを指定します。
v2	有効または無効にする SNMP バージョンを指定します。
v3	有効または無効にする SNMP バージョンを指定します。
enable	指定されたバージョンをイネーブルにします。
disable	指定されたバージョンをディセーブルにします。

コマンド デフォルト

デフォルトでは、すべての SNMP バージョンはイネーブルになっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、SNMP バージョン 1 をイネーブルにする例を示します。

```
(Cisco Controller) > config snmp version v1 enable
```

関連コマンド

show snmpversion

config tacacs acct

TACACS+アカウンティング サーバを設定するには、**config tacacs acct** コマンドを使用します。

config tacacs acct {**add***1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **server-timeout** *1-3 seconds*}

構文の説明

add	新しい TACACS+ アカウンティング サーバを追加します。
1 ～ 3	TACACS+ アカウンティング サーバ インデックスを 1 から 3 に指定します。
ip-addr	TACACS+ アカウンティング サーバの IPv4 または IPv6 アドレスを指定します。
port	TACACS+ サーバの TCP ポートを指定します。
ascii/hex	使用する TACACS+ サーバの秘密キーのタイプを指定します（ASCII または HEX）。
secret	秘密キーを ASCII 文字または 16 進数文字で指定します。
delete	TACACS+ サーバを削除します。
disable	TACACS+ サーバを無効にします。
enable	TACACS+ サーバを有効にします。
server-timeout	TACACS+ サーバのデフォルト サーバ タイムアウトを変更します。
seconds	TACACS+サーバがタイムアウトするまでの秒数を指定します。サーバ タイムアウトの範囲は 5 ～ 30 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、IPv4 アドレス 10.0.0.0、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ アカウンティング サーバ インデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs acct add 1 10.0.0.0 10 ascii 12345678
```

次に、IPv6 アドレス 2001:9:6:40::623、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ アカウンティング サーバ インデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs acct add 1  2001:9:6:40::623 10 ascii 12345678
```

次に、TACACS+ アカウンティング サーバのサーバ タイムアウトを5 秒間に設定する例を示します。

```
(Cisco Controller) > config tacacs acct server-timeout 1 5
```

config tacacs athr

TACACS+ 許可サーバを設定するには、**config tacacs athr** コマンドを使用します。

config tacacs athr {**add***1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **mgmt-server-timeout** *1-3 seconds* | **server-timeout** *1-3 seconds*}

構文の説明

add	新しい TACACS+ 許可サーバを追加します（IPv4 または IPv6）。
1 ～ 3	1 から 3 までの TACACS+ サーバ インデックス。
ip-addr	TACACS+ 許可サーバの IP アドレス（IPv4 または IPv6）。
port	TACACS+ サーバの TCP ポート。
ascii/hex	使用する秘密キーのタイプ（ASCII または HEX）。
secret	ASCII または HEX の文字による秘密キー。
delete	TACACS+ サーバを削除します。
disable	TACACS+ サーバを無効にします。
enable	TACACS+ サーバを有効にします。
mgmt-server-timeout *1-3seconds*	サーバのデフォルトの管理ログイン サーバ タイムアウトを変更します。サーバがタイムアウトするまでの秒数は 1 ~ 30 秒です。
server-timeout *1-3 seconds*	サーバのデフォルトのネットワーク ログイン サーバ タイムアウトを変更します。サーバがタイムアウトするまでの秒数は5~30秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。
8.0	このコマンドは、IPv4とIPv6の両方のアドレス形式をサポートします。

次に、IPv4 アドレス 10.0.0.0、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ 許可サーバ インデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs athr add 1 10.0.0.0 49 ascii 12345678
```

次に、IPv6 アドレス 2001:9:6:40::623、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ 許可サーバ インデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs athr add 1 2001:9:6:40::623 49 ascii 12345678
```

次に、TACACS+許可サーバの再送信タイムアウトを5秒間に設定する例を示します。

```
(Cisco Controller) > config tacacs athr server-timeout 1 5
```

config tacacs athr mgmt-server-timeout

管理ユーザのデフォルト TACACS+ 許可サーバのタイムアウトを設定するには、**config tacacs athr mgmt-server-timeout** コマンドを使用します。

config tacacs athr mgmt-server-timeout *index timeout*

構文の説明

index	TACACS+ 許可サーバ インデックス。
timeout	タイムアウト値。指定できる範囲は 1 ～ 30 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、管理ユーザのデフォルト TACACS+ 許可サーバのタイムアウトを設定する例を示します。

```
(Cisco Controller) > config tacacs athr mgmt-server-timeout 1 10
```

config tacacs auth

TACACS+ 認証サーバを設定するには、**config tacacs auth** コマンドを使用します。

config tacacs auth { **add** *1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **mgmt-server-timeout** *1-3 seconds* | **server-timeout** *1-3seconds* }

構文の説明

add	新しい TACACS+ アカウンティング サーバを追加します。
1 ～ 3	1 から 3 までの TACACS+ アカウンティング サーバ インデックス。
IP addr	TACACS+ アカウンティング サーバの IP アドレス。
port	TACACS+ アカウンティング サーバに使用するコントローラ ポート。
ascii/hex	使用する秘密キーのタイプ（ASCII または HEX）。
secret	ASCII または HEX の文字による秘密キー。
delete	TACACS+ サーバを削除します。
disable	TACACS+ サーバを無効にします。
enable	TACACS+ サーバを有効にします。
mgmt-server-timeout *1-3 seconds*	サーバのデフォルトの管理ログイン サーバ タイムアウトを変更します。サーバがタイムアウトするまでの秒数は 1 ~ 30 秒です。
server-timeout *1-3 seconds*	サーバのデフォルトのネットワーク ログイン サーバ タイムアウトを変更します。サーバがタイムアウトするまでの秒数は 5~30 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、IPv4 アドレス 10.0.0.3、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ 認証サーバ インデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs auth add 1 10.0.0.3 49 ascii 12345678
```

次に、IPv6 アドレス 2001:9:6:40::623、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ 認証サーバ インデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs auth add 1 2001:9:6:40::623 49 ascii 12345678
```

次に、TACACS+ 認証サーバのサーバ タイムアウトを設定する例を示します。

```
(Cisco Controller) > config tacacs auth server-timeout 1 5
```

config tacacs auth mgmt-server-timeout

管理ユーザのデフォルト TACACS+ 認証サーバのタイムアウトを設定するには、**config tacacs auth mgmt-server-timeout** コマンドを使用します。

config tacacs auth mgmt-server-timeout *index timeout*

構文の説明

index	TACACS+ 認証サーバ インデックス。
timeout	タイムアウト値。指定できる範囲は 1 ～ 30 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、管理ユーザのデフォルト TACACS+ 認証サーバのタイムアウトを設定する例を示します。

```
(Cisco Controller) > config tacacs auth mgmt-server-timeout 1 10
```

関連コマンド

config tacacs auth

config tacacs dns

DNS サーバから TACACS IP 情報を取得するには、**config radius dns** コマンドを使用します。

config radius dns {**global** *port* {*ascii* | *hex*} *secret* | **query** *url timeout* | **serverip** *ip_address* | **disable** | **enable**}

構文の説明

global	グローバル ポートおよび DNS サーバから TACACS IP 情報を取得する秘密キーを設定します。
port	認証用のポート番号。有効な範囲は 1 ～ 65535 です。すべての DNS サーバは同じ認証ポートを使用する必要があります。
ascii	ASCII に設定する必要のある共有秘密キーの形式。
hex	16 進数に設定する必要のある共有秘密キーの形式。
secret	TACACS サーバのログイン秘密。
query	TACACS サーバと DNS タイムアウトの完全修飾ドメイン名（FQDN）を設定します。
url	TACACS サーバの FQDN。FQDN は最大 63 文字の英数字（大文字と小文字を区別）で指定できます。
timeout	Cisco Wireless LAN Controller（WLC）がリクエストのタイムアウトを設定して再送信するまでの最大待機日数。指定できる範囲は 1 ～ 180 です。
serverip	DNS サーバの IP アドレスを設定します。
ip_address	DNS サーバの IP アドレス。
disable	TACACS DNS 機能を無効にします。デフォルトではディセーブルになっています。
enable	Cisco WLC が DNS サーバから TACACS IP 情報を取得できるようにします。

コマンド デフォルト

DNS サーバから TACACS IP 情報を取得することはできません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

アカウンティング ポートは認証ポートから取得されます。すべての DNS サーバは同じ秘密キーを使用する必要があります。DNS クエリを有効にすると、スタティック設定は上書きされます。DNS リストはスタティック AAA リストよりも優先されます。

次に、Cisco WLC で TACACS DNS 機能を有効にする例を示します。

```
(Cisco Controller) > config tacacs dns enable
```

config tacacs fallback-test interval

TACACS + プローブ間隔を設定するには、 **config tacacs fallback-test interval** コマンドを使用します。

config tacacs fallback-test interval { *seconds* }

構文の説明

seconds	TACACS+ プローブ間隔（秒単位）。無効は 0 で、範囲は 180 ～ 3600 秒です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.2	このコマンドは本リリースで追加されました。

次に、TACACS+ プローブ間隔を設定する例を示します。

```
(Cisco Controller) >  config tacacs fallback-test interval 200
```

config time manual

システムの時刻を設定するには、**config time manual** コマンドを使用します。

config time manual *MM* | *DD* | *YY HH*:*MM*:*SS*

構文の説明

MM/*DD*/*YY*	日付。
HH:*MM*:*SS*	時刻。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、システムの日付を 04/04/2010 に設定し、システムの時刻を 15:29:00 に設定する例を示します。

```
(Cisco Controller) > config time manual 04/04/2010 15:29:00
```

関連コマンド

show time

config time ntp

ネットワーク タイム プロトコル（NTP）を設定するには、**config time ntp** コマンドを使用します。

config time ntp {**auth** {**enable** *server-index key-index* | **disable** *server-index*} | **interval** *interval* | **key-auth** {**add** *key-index* **md5** {**ascii** | **hex**} *key*} | **delete** *key-index*} | **server** *index IP Address*}

構文の説明

auth	NTP 認証を設定します。
enable	NTP 認証をイネーブルにします。
server-index	NTP サーバ インデックス。
key-index	1 ～ 4294967295 のキー インデックス。
disable	NTP 認証をディセーブルにします。
interval	NTP バージョン 3 のポーリング間隔を設定します。
interval	NTP ポーリング間隔（秒）。有効範囲は 3600 ～ 604800 秒です。
key-auth	NTP 認証キーを設定します。
add	NTP 認証キーを追加します。
md5	認証プロトコルを指定します。
ascii	ASCII キー タイプを指定します。
hex	16 進数キー タイプを指定します。
key	最大 16 文字の ASCII キー形式または最大 32 桁の 16 進キー形式を指定します。
delete	NTP サーバを削除します。
server	NTP サーバを設定します。
IP Address	NTP サーバの IP アドレス。エントリを削除するには 0.0.0.0 または :: を使用します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

- コントローラに NTP サーバを追加するには、**config time ntp server** *index IP Address* コマンドを使用します。
- コントローラから NTP サーバ（IPv4）を削除するには、**config time ntp server** *index 0.0.0.0* コマンドを使用します。

  コントローラから NTP サーバ（IPv6）を削除するには、**config time ntp server** *index ::* コマンドを使用します。
- コントローラ上で設定されている NTP サーバを表示するには、**show time**コマンドを使用します。

次に、NTP のポーリング間隔を 7000 秒に設定する例を示します。

```
(Cisco Controller) > config time ntp interval 7000
```

次に、サーバ インデックスが 4 で、キー インデックスが 1 である NTP 認証をイネーブルにする例を示します。

```
(Cisco Controller) > config time ntp auth enable 4 1
```

次に、キー形式が 16 進数文字で、キー インデックスが 1 である、値が ff の NTP 認証キーを追加する例を示します。

```
(Cisco Controller) > config time ntp key-auth add 1 md5 hex ff
```

次に、キー形式が ASCII 文字で、キー インデックスが 1 である、値が ff の NTP 認証キーを追加する例を示します。

```
(Cisco Controller) > config time ntp key-auth add 1 md5 ascii ciscokey
```

次に、NTP サーバを追加し、コントローラに設定されているサーバを表示する例を示します。

```
(Cisco Controller) > config time ntp server  1 10.92.125.52
(Cisco Controller) > config time ntp server  2 2001:9:6:40::623
(Cisco Controller) > show time
Time.......................................... Fri May 23 12:04:18 2014

Timezone delta................................ 0:0
Timezone location............................. (GMT +5:30) Colombo, New Delhi, Chennai,
 Kolkata
```

```
NTP Servers
NTP Polling Interval..................... 3600

Index NTP Key Index  NTP Server NTP    Msg Auth Status
------- ------------------------------------------------
1            1      10.92.125.52       AUTH SUCCESS
2            1      2001:9:6:40::623   AUTH SUCCESS
```

次に、NTP サーバを削除し、NTPサーバ リストからそのサーバが削除されていることを確認する例を示します。

```
(Cisco Controller) > config time ntp server  1 0.0.0.0
(Cisco Controller) > config time ntp server  2 ::
(Cisco Controller) > show time
Time..................................... Fri May 23 12:04:18 2014

Timezone delta..................................... 0:0
Timezone location.............................. (GMT +5:30) Colombo, New Delhi, Chennai,
 Kolkata

NTP Servers
NTP Polling Interval..................... 3600

Index NTP Key Index  NTP Server NTP    Msg Auth Status
------- ------------------------------------------------
```

config time timezone

システムのタイム ゾーンを設定するには、**config time timezone** コマンドを使用します。

config time timezone {**enable** | **disable**} *delta_hours delta_mins*

構文の説明

enable	夏時間をイネーブルにします。
disable	夏時間をディセーブルにします。
delta_hours	Universal Coordinated Time（UCT）からのローカル時間の差。
delta_mins	UCT からのローカル分の差。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、夏時間をイネーブルにする例を示します。

```
(Cisco Controller) > config time timezone enable 2 0
```

関連コマンド

show time

config time timezone location

適切な時期が来たら自動的に夏時間が設定されるようにタイムゾーンの場所を設定するには、**config time timezone location** コマンドを使用します。

config time timezone location *location_index*

構文の説明	*location_index*

必要な時間帯を表す番号。時間帯は次のとおりです。

- （GMT-12:00）日付変更線、西側
- （GMT-11:00）サモア
- （GMT-10:00）ハワイ
- （GMT-9:00）アラスカ
- （GMT-8:00）太平洋標準時（米国およびカナダ）
- （GMT-7:00）山岳部標準時（米国およびカナダ）
- （GMT-6:00）中央標準時（米国およびカナダ）
- （GMT-5:00）東部標準時（米国およびカナダ）
- （GMT-4:00）大西洋標準時（カナダ）
- （GMT-3:00）ブエノスアイレス（アルゼンチン）
- （GMT-2:00）中部大西洋
- （GMT-1:00）アゾレス諸島
- （GMT）ロンドン、リスボン、ダブリン、エディンバラ（デフォルト値）
- （GMT+1:00）アムステルダム、ベルリン、ローマ、ウィーン
- （GMT+2:00）エルサレム
- （GMT+3:00）バグダッド
- （GMT+4:00）マスカット、アブダビ
- （GMT+4:30）カブール
- （GMT+5:00）カラチ、イスラマバード、タシュケント
- （GMT+5:30）コロンボ、コルカタ、ムンバイ、ニューデリー
- （GMT+5:45）カトマンズ
- （GMT+6:00）アルマトイ、ノボシビルス

ク

- （GMT+6:30）ラングーン
- （GMT+7:00）サイゴン、ハノイ、バンコク、ジャカルタ
- （GMT+8:00）香港、北京、重慶
- （GMT+9:00）東京、大阪、札幌
- （GMT+9:30）ダーウィン
- （GMT+10:00）シドニー、メルボルン、キャンベラ
- （GMT+11:00）マガダン、ソロモン諸島、ニューカレドニア
- （GMT+12:00）カムチャツカ、マーシャル諸島、フィジー
- （GMT+12:00）オークランド（ニュージーランド）

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、夏時間が場所インデックス10に自動的に設定されるようにタイムゾーンの場所を設定する例を示します。

```
(Cisco Controller) > config time timezone location 10
```

関連コマンド

show time

config trapflags 802.11-Security

802.11 セキュリティ関連トラップの送信を有効または無効にするには、**config trapflags 802.11-Security** コマンドを使用します。

config trapflags 802.11-Security wepDecryptError {**enable** | **disable**}

構文の説明

enable	802.11 セキュリティ関連トラップの送信をイネーブルにします。
disable	802.11セキュリティ関連トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、802.11 セキュリティ関連トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11 セキュリティ関連トラップをディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags 802.11-Security wepDecryptError disable
```

関連コマンド

show trapflags

config trapflags aaa

AAA サーバ関連トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags aaa** コマンドを使用します。

config trapflags aaa {**auth** | **servers**} {**enable** | **disable**}

構文の説明

auth	管理ユーザ、ネットユーザ、またはMACフィルタにAAA認証エラーが発生した場合に、トラップの送信をイネーブルにします。
servers	RADIUS サーバが応答していない場合に、トラップの送信をイネーブルにします。
enable	AAA サーバ関連トラップの送信をイネーブルにします。
disable	AAA サーバ関連トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、AAA サーバ関連トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、AAA サーバ関連トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags aaa auth enable
```

関連コマンド

show watchlist

config trapflags adjchannel-rogueap

隣接チャネルで不正なアクセス ポイントが検出された場合に、トラップ通知を設定するには、**config trapflags adjchannel-rogueap** コマンドを使用します。

config trapflags adjchannel-rogueap {**enable** | **disable**}

構文の説明

enable	隣接チャネルで不正なアクセス ポイントが検出された場合に、トラップ通知をイネーブルにします。
disable	隣接チャネルで不正なアクセス ポイントが検出された場合に、トラップ通知をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、隣接チャネルで不正なアクセス ポイントが検出された場合に、トラップ通知をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags adjchannel-rogueap enable
```

関連コマンド

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags strong-pwdcheck

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags ap

Cisco Lightweight アクセス ポイント関連トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags ap** コマンドを使用します。

config trapflags ap {**register** | **interfaceUp**} {**enable** | **disable**}

構文の説明

register	Cisco Lightweight アクセス ポイントが Cisco スイッチに登録する場合に、トラップの送信をイネーブルにします。
interfaceUp	Cisco Lightweight アクセス ポイント インターフェイス（A または B）が表示された場合に、トラップの送信をイネーブルにします。
enable	アクセスポイント関連トラップの送信をイネーブルにします。
disable	アクセス ポイント関連トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、Cisco Lightweight アクセス ポイント関連トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、トラップで、アクセス ポイント関連トラップの送信が行われないようにする例を示します。

```
(Cisco Controller) > config trapflags ap register disable
```

関連コマンド

show trapflags

config trapflags authentication

無効な SNMP アクセス権を持つトラップ送信をイネーブルまたはディセーブルにするには、**config trapflags authentication** コマンドを使用します。

config trapflags authentication {**enable** | **disable**}

構文の説明

enable	無効な SNMP アクセス権を持つトラップの送信をイネーブルにします。
disable	無効な SNMP アクセス権を持つトラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、無効な SNMP アクセス権を持つトラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、無効な SNMP アクセス権で、トラップの送信を行えないようにする例を示します。

```
(Cisco Controller) > config trapflags authentication disable
```

関連コマンド

show trapflags

config trapflags client

クライアント関連DOT11 トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags client** コマンドを使用します。

config trapflags client {**802.11-associate 802.11-disassociate** | **802.11-deauthenticate** | **802.11-authfail** | **802.11-assocfail** | **authentication** | **excluded**} {**enable** | **disable**}

構文の説明

802.11-associate	クライアントへの Dot11 アソシエーション トラップの送信をイネーブルにします。
802.11-disassociate	クライアントへのDot11ディスアソシエーション トラップの送信をイネーブルにします。
802.11-deauthenticate	クライアントへの Dot11 認証解除トラップの送信をイネーブルにします。
802.11-authfail	クライアントへの Dot11 認証エラー トラップの送信をイネーブルにします。
802.11-assocfail	クライアントへの Dot11 アソシエーション エラー トラップの送信をイネーブルにします。
authentication	クライアントへの認証成功トラップの送信をイネーブルにします。
excluded	除外したトラップのクライアントへの送信をイネーブルにします。
enable	クライアント関連DOT11 トラップの送信をイネーブルにします。
disable	クライアント関連 DOT11 トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、クライアント関連 DOT11 トラップの送信はディセーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、クライアントへの Dot11 アソシエーション解除トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags client 802.11-disassociate enable
```

関連コマンド **show trapflags**

config trapflags client max-warning-threshold

コントローラに関連付けるクライアントの数のしきい値を設定し、その後、SNMP トラップと syslog メッセージがコントローラに送信されるようにするには、**config trapflags client max-warning-threshold** コマンドを使用します。

config trapflags client max-warning-threshold {**threshold** | **enable** | **disable**}

構文の説明

threshold	コントローラに関連付けるクライアントの数のしきい値パーセントを設定し、その後、SNMP トラップと syslog メッセージがコントローラに送信されるようにします。範囲は 80 ～ 100 です。 2 つの警告の間の最小間隔は 10 分間です。この間隔を設定することはできません。
enable	トラップと syslog メッセージの生成をイネーブルにします。
disable	トラップと syslog メッセージの生成をディセーブルにします。

コマンド デフォルト

コントローラに関連付けられているクライアント数のデフォルトのしきい値は 90 % です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラに関連付けられているクライアント数のしきい値を設定する例を示します。

```
(Cisco Controller) > config trapflags client max-warning-threshold 80
```

関連コマンド

show trapflags

config trapflags client

config trapflags configsave

設定保存トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags configsave** コマンドを使用します。

config trapflags configsave {**enable** | **disable**}

構文の説明

enable	設定保存トラップの送信をイネーブルにします。
disable	設定保存トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、設定保存トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、設定保存トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags configsave enable
```

関連コマンド

show trapflags

config trapflags IPsec

IPSec トラップの送信を有効または無効にするには、**config trapflags IPsec** コマンドを使用します。

config trapflags IPsec {**esp-auth** | **esp-reply** | **invalidSPI** | **ike-neg** | **suite-neg** | **invalid-cookie**} {**enable** | **disable**}

構文の説明

esp-auth	ESP 認証エラーが発生したときに、IPSec トラップを送信できるようにします。
esp-reply	ESP 再送エラーが発生したときに、IPSec トラップの送信をイネーブルにします。
invalidSPI	ESP で無効な SPI が検出されたときに、IPSec トラップの送信をイネーブルにします。
ike-neg	IKE ネゴシエーション エラーが発生したときに、IPSec トラップの送信をイネーブルにします。
suite-neg	スイート ネゴシエーション エラーが発生したときに、IPSec トラップの送信をイネーブルにします。
invalid-cookie	Isakamp で無効なクッキーが検出されたときに、IPSec トラップの送信をイネーブルにします。
enable	IPSec トラップの送信をイネーブルにします。
disable	IPSec トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、IPSec トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ESP 認証エラーが発生したときに、IPSec トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags IPsec esp-auth enable
```

関連コマンド **show trapflags**

config trapflags linkmode

Cisco ワイヤレス LAN コントローラのレベル リンクのアップ/ダウン トラップ フラグをイネーブルまたはディセーブルにするには、**config trapflags linkmode** コマンドを使用します。

config trapflags linkmode {**enable** | **disable**}

構文の説明

enable	これにより、Cisco ワイヤレス LAN コントローラのレベル リンクのアップ/ダウン トラップ フラグをイネーブルにします。
disable	これにより、Cisco ワイヤレス LAN コントローラのレベル リンクのアップ/ダウン トラップ フラグをディセーブルにします。

コマンド デフォルト

デフォルトでは、Cisco WLC のレベル リンクのアップ/ダウン トラップ フラグはイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco ワイヤレス LAN コントローラのレベル リンクのアップ/ダウン トラップをイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags linkmode disable
```

関連コマンド

show trapflags

config trapflags mesh

メッシュ アクセス ポイントが検出された場合に、トラップ通知を設定するには、**config trapflags mesh** コマンドを使用します。

config trapflags mesh {**enable** | **disable**}

構文の説明

enable	メッシュ アクセス ポイントが検出された場合に、トラップ通知をイネーブルにします。
disable	メッシュ アクセス ポイントが検出された場合に、トラップ通知をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メッシュ アクセス ポイントが検出された場合に、トラップ通知をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags mesh enable
```

関連コマンド

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags strong-pwdcheck

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags multiusers

複数ログインがアクティブな場合にトラップ送信をイネーブルまたはディセーブルにするには、**config trapflags multiusers** コマンドを使用します。

config trapflags multiusers {**enable** | **disable**}

構文の説明

enable	複数ログインがアクティブな場合に、トラップ送信をイネーブルにします。
disable	複数ログインがアクティブな場合に、トラップ送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、複数ログインがアクティブな場合、トラップ送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、複数ログインがアクティブな場合に、トラップ送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags multiusers disable
```

関連コマンド

show trapflags

config trapflags rfid

電波による個体識別（RFID）タグの最大数のしきい値を設定し、その後、SNMP トラップと syslog メッセージをコントローラに送信するには、**config trapflags rfid** コマンドを使用します。

config trapflags rfid {**threshold** | **enable** | **disable**}

構文の説明

threshold	RFID タグの最大数のしきい値パーセントを設定し、その後、SNMP トラップと syslog メッセージがコントローラに送信されるようにします。範囲は 80 ～ 100 です。 トラップと syslog メッセージが 10 分ごとに生成されます。この間隔は設定できません。
enable	トラップと syslog メッセージの生成をイネーブルにします。
disable	トラップと syslog メッセージの生成をディセーブルにします。

コマンド デフォルト

RFID タグの最大数のデフォルトのしきい値は、90% です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

次の表に、異なるコントローラでサポートされる RFID タグの最大数を示します。

表 *9:* 異なるコントローラでサポートされる *RFID* タグの最大数

コントローラ	サポートされているクライアントの最大数
Cisco 5500 シリーズ コントローラ	5000
Cisco 2500 シリーズ コントローラ	500
Cisco ワイヤレス サービス モジュール 2	10000
Cisco Flex 7500 シリーズ コントローラ	50000
Cisco 8500 シリーズ コントローラ	50000
Cisco Virtual Wireless LAN Controller	3000

次に、RFID タグの最大数のしきい値を設定する例を示します。

```
(Cisco Controller) > config trapflags rfid 80
```

関連コマンド

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags strong-pwdcheck

config trapflags rogueap

config trapflags mesh

show trapflags

config trapflags rogueap

不正なアクセス ポイント検出トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags rogueap** コマンドを使用します。

config trapflags rogueap {**enable** | **disable**}

構文の説明

enable	不正なアクセス ポイント検出トラップの送信をイネーブルにします。
disable	不正なアクセス ポイント検出トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、不正なアクセス ポイント検出トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、不正なアクセス ポイント検出トラップの送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags rogueap disable
```

関連コマンド

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show trapflags

config trapflags rrm-params

無線リソース管理（RRM）パラメータ トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags rrm-params** コマンドを使用します。

config trapflags rrm-params {**tx-power** | **channel** | **antenna**} {**enable** | **disable**}

構文の説明

tx-power	RF マネージャが Cisco Lightweight アクセス ポイント インターフェイスの tx パワー レベルを自動的に変更する場合に、トラップの送信をイネーブルにします。
channel	RF マネージャが Cisco Lightweight アクセス ポイント インターフェイスのチャネルを自動的に変更する場合に、トラップの送信をイネーブルにします。
antenna	RF マネージャが Cisco Lightweight アクセス ポイント インターフェイスのアンテナを自動的に変更する場合に、トラップの送信をイネーブルにします。
enable	RRM パラメータ関連トラップの送信をイネーブルにします。
disable	RRM パラメータ関連トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、RRM パラメータ トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RRM パラメータ関連トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags rrm-params tx-power enable
```

関連コマンド

show trapflags

config trapflags rrm-profile

無線リソース管理（RRM）プロファイル関連トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags rrm-profile** コマンドを使用します。

config trapflags rrm-profile {**load** | **noise** | **interference** | **coverage**} {**enable** | **disable**}

構文の説明

load	RFマネージャによって管理されるロードプロファイルが失敗した場合に、トラップの送信をイネーブルにします。
noise	RFマネージャによって管理されるノイズプロファイルが失敗した場合に、トラップの送信をイネーブルにします。
interference	RF マネージャによって管理されるインターフェイス プロファイルが失敗した場合に、トラップの送信をイネーブルにします。
coverage	RFマネージャによって管理されるカバレッジプロファイルが失敗した場合に、トラップの送信をイネーブルにします。
enable	RRM プロファイル関連トラップの送信をイネーブルにします。
disable	RRMプロファイル関連トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、RRM プロファイル関連トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RRM プロファイル関連トラップの送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags rrm-profile load disable
```

関連コマンド

show trapflags

config trapflags stpmode

スパニングツリー トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags stpmode** コマンドを使用します。

config trapflags stpmode {**enable** | **disable**}

構文の説明

enable	スパニングツリー トラップの送信をイネーブルにします。
disable	スパニングツリー トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、スパニングツリー トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、スパニングツリー トラップの送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags stpmode disable
```

関連コマンド

show trapflags

config trapflags strong-pwdcheck

強力なパスワードのチェック用のトラップ通知を設定するには、**config trapflags strong-pwdcheck** コマンドを使用します。

config trapflags strong-pwdcheck {**enable** | **disable**}

構文の説明

enable	強力なパスワードのチェック用のトラップ通知をイネーブルにします。
disable	強力なパスワードのチェック用のトラップ通知をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、強力なパスワード チェック用のトラップ通知をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags strong-pwdcheck enable
```

関連コマンド

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags wps

Wireless Protection System（WPS）トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags wps** コマンドを使用します。

config trapflags wps {**enable** | **disable**}

構文の説明

enable	WPS トラップの送信をイネーブルにします。
disable	WPS トラップの送信をディセーブルにします。

コマンド デフォルト

デフォルトでは、 WPS トラップの送信はイネーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WPS トラップの送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags wps disable
```

関連コマンド

show trapflags

config tunnel eogre heart-beat

キープアライブ ping 間隔を設定するには、 **config tunnel eogre** コマンドを使用します。

config tunnel eogre heart-beat {**interval** | **max-skip-count**} *number-value*

構文の説明

interval *number-value*	エコー要求メッセージ間の間隔（秒単位）。
max-skip-count *number-value*	メンバーが機能していないと見なすまでの最大再試行回数。

コマンド デフォルト

ハートビート *interval* のデフォルト値は 60 秒です。範囲は 10 ～ 600 秒です。

ハートビート *max-skip-count* のデフォルト値は 3 回の再試行です。範囲は、3 ～ 10 回の再試行です。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、ハートビート間隔の値を 45 秒に設定する例を示します。

```
config tunnel eogre heart-beat interval 45
```

config tunnel eogre gateway

GRE ゲートウェイの IPv4 アドレス経由でイーサネットを設定するには、 **config tunnel eogre gateway** コマンドを使用します。

config tunnel eogre gateway {{{**add** | **modify**} *gateway-name* {**ipv4-address** | **ipv6-address**} *gateway-ip-address*} | {**delete** *gateway-name*}}

構文の説明

add	新しいゲートウェイを追加します。
delete	ゲートウェイを削除します。
modify	既存のゲートウェイを変更します。
ipv4-address	ゲートウェイの IPv4 アドレスを入力します。
ipv6-address	ゲートウェイの IPv6 アドレスを入力します。
gateway-ip-address	ゲートウェイの IPv4 または IPv6 アドレスです。
gateway-name	トンネル ゲートウェイ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。
8.3	トンネル ゲートウェイの IPv6 アドレス形式のオプションが追加されました。

- IPv4 アドレスの例

```
config tunnel eogre gateway add hurricane ipv4 192.168.10.1
```

- IPv6 アドレスの例

```
config tunnel eogre gateway add hurricane ipv6 2001:DB8::1
```

config tunnel eogre domain

トンネル ゲートウェイ ドメイン構成を実行するには、**config tunnel eogre domain** コマンドを使用します。

config tunnel eogre domain {{**create** | **delete**}*domain-name*} {**add** | **remove**}*domain-name gateway-name*

構文の説明

create	新しいゲートウェイ ドメイン名を作成します。
delete	ゲートウェイ ドメインを削除します。
add	ゲートウェイ名をドメインに追加します
remove	ドメインからゲートウェイ名を削除します
domain-name	ドメイン名
gateway-name	ゲートウェイ名

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、新しいドメイン名を作成する例を示します。

```
config tunnel eogre domain create web.com data
```

config tunnel profile

プロファイルを作成、コピーまたは削除するには、**config tunnel profile** コマンドを使用します。

config tunnel profile {**copy** | **create** | **delete**} *profile-name*

構文の説明

copy	既存のプロファイルをコピーします。
create	新しいプロファイルを作成します。
delete	既存のプロファイルを削除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、新しいプロファイルを作成する例を示します。

```
config tunnel profile create floorone
```

config tunnel profile_rule

プロファイルにルールを追加したりルールを変更するには、**config tunnel profile** コマンドを使用します。

config tunnel profile rule {**add** | **modify** }*profile-name* **realm-filter** *realm-string* **eogre vlan** *vlan-id gateway-domain-name*

構文の説明

add	新規ルールを追加します。
modify	既存のルールを変更します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、プロファイルにルールを追加する例を示します。

```
config tunnel profile add table realm filter 5 eogre vlan 3 web.com
```

config tunnel profile_rule-delete

プロファイルからルールを削除するには、**config tunnel profile** コマンドを使用します。

config tunnel profile ruledelete *profile-name* **realm-filter** *realm-string*

構文の説明	**delete** プロファイルから既存のルールを削除します。

コマンド デフォルト	なし

コマンド履歴	リリース	変更内容
	8.1	このコマンドが導入されました。

次に、プロファイルからルールを削除する例を示します。

```
config tunnel profile delete table realm filter 5
```

config tunnel profile eogre-DHCP82

DHCP オプション 82 パラメータを有効または無効にするには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **DHCP-Opt-82** {**enable** | **disable**}

構文の説明

enable	システムの DHCP オプション 82 パラメータを有効にします。
disable	システムの DHCP オプション 82 パラメータを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、DHCP オプション 82 パラメータを有効にする例を示します。

```
config tunnel profile eogre test dhcp-opt-82 enable
```

config tunnel profile eogre-gateway-radius-proxy

ゲートウェイ Radius プロキシを有効または無効にするには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **gateway-radius-proxy** {**enable** | **disable**}

構文の説明

enable	Radius プロキシとしてゲートウェイを有効にします。
disable	Radius のプロキシとしてゲートウェイを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、ゲートウェイ プロキシを有効にする例を示します。

```
config tunnel profile eogre test gateway-radius-proxy enable
```

config tunnel profile eogre-gateway-radius-proxy-accounting

アカウンティング Radius プロキシとしてゲートウェイを有効または無効にするには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **gateway-radius-proxy accounting** {**enable** | **disable**}

構文の説明

enable	アカウンティング Radius プロキシとしてゲートウェイを有効にします。
disable	アカウンティング Radius プロキシとしてゲートウェイを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、アカウンティング Radius プロキシとしてゲートウェイを無効にする例を示します。

```
config tunnel profile eogre test gateway-radius-proxy accounting disable
```

config tunnel profile eogre-DHCP82

DHCP オプション 82 パラメータを有効または無効にするには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **DHCP-Opt-82** {**enable** | **disable**}

構文の説明

enable	システムの DHCP オプション 82 パラメータを有効にします。
disable	システムの DHCP オプション 82 パラメータを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、DHCP オプション 82 パラメータを有効にする例を示します。

```
config tunnel profile eogre test dhcp-opt-82 enable
```

config tunnel profile eogre-DHCP82-circuit-id

DHCP オプション 82 パラメータで回路 ID フィールドの形式を設定するには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **DHCP-Opt-82 circuit-id** *parameter-id*

構文の説明

circuit-id	DHCPオプション 82 の回路 ID フィールドの形式を設定します
parameter-id	サポートされているパラメータのリスト。 • ap-mac • ap-ethmac • ap-name • ap-group-name • flex-group-name • ap-location • vlan-id • SSID-name • SSID-TYPE • Client-mac

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、DHCP オプション 82 パラメータで回路 ID の形式を設定する例を示します。

```
config tunnel profile eogre test dhcp-opt-82 circuit-id access1bldg
```

config tunnel profile eogre-DHCP82-delimiter

DHCP オプション 82 パラメータのデリミタ（区切り文字）を設定するには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **DHCP-Opt-82 delimiter** *delimiter character*

構文の説明

delimiter	システムの DHCP オプション 82 パラメータの区切り文字を設定します。
delimiter character	区切り文字は DHCP オプション 82 パラメータを区切るために使用されます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、DHCP オプション 82 パラメータを区切り文字で分割する例を示します。

```
config tunnel profile eogre test dhcp-opt-82 delimiter -
```

config tunnel profile eogre-DHCP82-format

DCHP オプション 82 で必要な形式を設定するには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **dhcp-opt-82 format** {**binary** | **ascii**}

構文の説明

binary	DHCPオプション82の形式をバイナリに設定します
ascii	DHCPオプション 82 の形式を Ascii に設定します

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、DHCPオプション 82 パラメータに「バイナリ」形式を設定する例を示します。

```
config tunnel profile eogre test dhcp-opt-82 format binary
```

config tunnel profile eogre-DHCP82-remote-id

DHCP オプション 82 パラメータでリモート ID フィールドの形式を設定するには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **DHCP-Opt-82 remote-id** *parameter-id*

構文の説明

remote-id	DHCPオプション 82 のリモート ID フィールドの形式を設定します
parameter-id	サポートされているパラメータのリスト。 • ap-mac • ap-ethmac • ap-name • ap-group-name • flex-group-name • ap-location • vlan-id • SSID-name • SSID-TYPE • Client-mac

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、DHCP オプション 82 パラメータでリモート ID の形式を設定する例を示します。

```
config tunnel profile eogre test dhcp-opt-82 remote-id access1flr
```

config watchlist add

無線LANの監視リストエントリを追加するには、**config watchlist add** コマンドを使用します。

config watchlist add {**mac** *MAC* | **username** *username*}

構文の説明

mac *MAC*	無線 LAN の MAC アドレスを指定します。
username *username*	監視するユーザの名前を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレス a5:6b:ac:10:01:6b で監視リスト エントリを追加する例を示します。

```
(Cisco Controller) >config watchlist add mac a5:6b:ac:10:01:6b
```

config watchlist delete

無線 LAN の監視リスト エントリを削除するには、**config watchlist delete** コマンドを使用します。

config watchlist delete {**mac** *MAC* | **username** *username*}

構文の説明

mac *MAC*	リストから削除する無線 LAN の MAC アドレスを指定します。
username *username*	リストから削除するユーザの名前を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレス a5:6b:ac:10:01:6b で監視リスト エントリを削除する例を示します。

```
(Cisco Controller) >config watchlist delete mac a5:6b:ac:10:01:6b
```

config watchlist disable

クライアントの監視リストを無効にするには、**config watchlist disable** コマンドを使用します。

config watchlist disable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントの監視リストをディセーブルにする例を示します。

```
(Cisco Controller) >config watchlist disable
```

config watchlist enable

無線 LAN の監視リスト エントリを有効にするには、**config watchlist enable** コマンドを使用します。

config watchlist enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、監視リスト エントリをイネーブルにする例を示します。

```
(Cisco Controller) >config watchlist enable
```

config wgb vlan

VLAN ワークグループブリッジ（WGB）クライアントのサポートを設定するには、**config wgb vlan** コマンドを使用します。

config wgb vlan {**enable** | **disable**}

構文の説明

enable	WGB の背後にある有線クライアントをデータ管理ゾーン（DMZ）のアンカー コントローラに接続できるようにします。
disable	WGB の背後にある有線クライアントを DMZ のアンカー コントローラへの接続から無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、VLAN WGB クライアントのサポートを有効にする例を示します。

```
(Cisco Controller) >config wgb vlan enable
```

config wlan

無線 LAN を作成、削除、イネーブル、またはディセーブルにするには、**config wlan** コマンドを使用します。

config wlan {**enable** | **disable** | **create** | **delete**} *wlan_id* [*name* | **foreignAp** *name ssid* | **all**]

構文の説明

enable	ワイヤレス LAN をイネーブルにします。
disable	ワイヤレス LAN をディセーブルにします。
create	無線 LAN を作成します。
delete	無線 LAN を削除します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
name	（任意）最大 32 文字の英数字の WLAN プロファイル名。
foreignAp	（任意）サードパーティのアクセス ポイント設定を指定します。
ssid	最大 32 文字の英数字の SSID（ネットワーク名）。
all	（任意）すべての無線 LAN を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config wlan create コマンドを使用して新しい WLAN を作成すると、無効モードで作成されます。設定が終了するまでは、無効のままにしてください。

SSID を指定しない場合は、プロファイル名パラメータがプロファイル名と SSID の両方に使用されます。

管理インターフェイスおよび AP マネージャ インターフェイスが同じポートにマップされており、いずれも同じ VLAN のメンバである場合は、WLAN を無効にしてから、ポートマッピングをいずれかのインターフェイスに変更する必要があります。管理インターフェイスと AP マネージャ インターフェイスが別々の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。

アクセス ポイント グループに割り当てられている WLAN を削除しようとすると、エラー メッセージが表示されます。そのまま続行すると、アクセス ポイント グループとアクセス ポイントの無線から WLAN が削除されます。

次に、無線 LAN 識別子 16 をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan enable 16
```

config wlan 7920-support

電話に対するサポートを設定するには、**config wlan 7920-support** コマンドを使用します。

config wlan 7920-support {**client-cac-limit** | **ap-cac-limit**} {**enable** | **disable**} *wlan_id*

構文の説明

ap-cac-limit	クライアント制御のコール アドミッション制御（CAC）を必要とする（シスコのベンダー固有情報要素（IE）が要求される）電話をサポートします。
client-cac-limit	アクセス ポイント制御の CAC を必要とする（IEEE 802.11e Draft 6 QBSS-load が要求される）電話をサポートします。
enable	電話サポートをイネーブルにします。
disable	電話サポートをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

1 つの WLAN で、WMM モードとクライアントにより制御された CAC モードの両方を有効にすることはできません。

次に、無線 LAN ID 8 で、クライアント制御される CAC を必要とする電話サポートをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan 7920-support ap-cac-limit enable 8
```

config wlan 802.11e

無線 LAN で 802.11e サポートを設定するには、**config wlan 802.11e** コマンドを使用します。

config wlan 802.11e {**allow** | **disable** | **require**} *wlan_id*

構文の説明

allow	無線 LAN で 802.11e 対応クライアントを許可します。
disable	無線 LAN で 802.11e サポートをディセーブルにします。
require	無線 LAN で 802.11e 対応クライアントを要求します。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

802.11e は LAN アプリケーションに Quality of Service（QoS）サポートを提供します。これは、Voice over Wireless IP（VoWIP）など遅延に影響されやすいアプリケーションにとって重要なサポートです。

802.11e は 802.11 メディア アクセス コントロール レイヤ（MAC レイヤ）の拡張版であり、調整済時分割多元接続（TDMA）が設定され、音声やビデオなど遅延に影響されやすいアプリケーション向けのエラー修正メカニズムが追加されています。802.11e 仕様は特にマルチメディア機能が組み込まれたネットワークでの使用に適しており、シームレスな相互運用性を実現します。

次に、LAN ID 1 の無線 LAN で 802.11e を許可する例を示します。

```
(Cisco Controller) >config wlan 802.11e allow 1
```

config wlan aaa-override

無線 LAN で AAA を介したユーザ ポリシー オーバーライドを設定するには、**config wlan aaa-override** コマンドを使用します。

config wlan aaa-override {**enable** | **disable**} {*wlan_id* | **foreignAp**}

構文の説明

enable	ポリシー オーバーライドをイネーブルにします。
disable	ポリシー オーバーライドをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

AAA はディセーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

AAA オーバーライドが有効になっていて、クライアントで AAA と Cisco Wireless LAN Controller の無線 LAN 認証パラメータが競合している場合、クライアント認証は AAA サーバによって行われます。この認証の一環として、オペレーティング システムはクライアントをデフォルトの Cisco Wireless LAN VLAN から、AAA サーバによって返されたコントローラのインターフェイス構成（MAC フィルタリング、802.1X、および Wi-Fi Protected Access（WPA）動作に対してだけ設定されている場合）で事前定義された VLAN に移動します。すべてのケースで、コントローラのインターフェイス構成で事前定義されている限り、オペレーティング システムは QoS、DSCP、802.1p 優先順位タグ値および AAA サーバで指定された ACLs を使用します（この AAA オーバーライドによる VLAN スイッチングは、ID ネットワーキングとも呼ばれます）。

企業の無線 LAN が VLAN 2 に割り当てられている管理インターフェイスを使用し、AAA オーバーライドが VLAN 100 へのリダイレクトを返す場合、VLAN 100 が割り当てられている物理ポートに関係なく、オペレーティング システムはすべてのクライアント送信を VLAN 100 にリダイレクトします。

AAA Override をディセーブルにすると、コントローラの認証パラメータ設定がすべてのクライアント認証においてデフォルトで使用され、コントローラ無線 LAN にクライアント固有の認証パラメータがない場合は、AAA サーバのみによって認証が実行されます。

AAA オーバーライド値は、RADIUS サーバから取り込まれる場合があります。

次に、WLAN ID 1 で AAA を介したユーザ ポリシー オーバーライドを設定する例を示します。

```
(Cisco Controller) >config wlan aaa-override enable 1
```

config wlan acl

無線 LAN のアクセス コントロール リスト（ACL）を設定するには、**config wlan acl** コマンドを使用します。

config wlan acl ［*acl_name* | **none**］

構文の説明

wlan_id	無線 LAN 識別子（1～512）。
acl_name	（任意）ACL 名です。
none	（任意）指定された無線 LAN の ACL 設定をクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 1 と office_1 という名前の ACL で WLAN アクセス コントロール リストを設定する例を示します。

```
(Cisco Controller) >config wlan acl 1 office_1
```

config wlan apgroup

アクセス ポイント グループの VLAN 機能を管理するには、**config wlan apgroup** コマンドを使用します。

config wlan apgroup {**add** *apgroup_name* [*description*] | **delete** *apgroup_name* | **description** *apgroup_name description* | **interface-mapping** {**add** | **delete**} *apgroup_name wlan_id interface_name* | **nac-snmp** {**enable** | **disable**} *apgroup_name wlan_id* | **nasid** *NAS-ID apgroup_name* | **profile-mapping** {**add** | **delete**} *apgroup_nameprofile_name* | **wlan-radio-policy** *apgroup_namewlan-id* {**802.11a-only** | **802.11bg** | **802.11g-only** | **all**} | **hotspot** {**venue** {**type** *apgroup_namegroup_codetype_code* | **name** *apgroup_namelanguage_codevenue_name*} | **operating-class** {**add** | **delete**} *apgroup_nameoperating_class_value*}}

構文の説明

add	新しいアクセスポイントグループ（APグループ）を作成します。
apgroup_name	アクセス ポイント グループ名。
wlan_id	1 ～ 512 の無線 LAN 識別子。
delete	AP グループから無線 LAN を除外します。
description	AP グループについて説明します。
description	AP グループの説明。
interface-mapping	（任意）AP グループから無線 LAN を割り当てるか削除します。
interface_name	（任意）AP グループをマップするインターフェイス。
nac-snmp	特定の AP グループの NAC SNMP 機能を設定します。アクセス ポイント グループでの Network Admission Control（NAC）アウトオブバンド サポートをイネーブルまたはディセーブルにします。
enable	AP グループ上で NAC アウトオブバンドのサポートをイネーブルにします。
disable	AP グループ上で NAC アウトオブバンドのサポートをディセーブルにします。

NAS-ID	AP グループのネットワーク アクセス サーバ ID（NAS-ID）。NAS-ID は、認証要求を使用してコントローラによって（RADIUS クライアントとして）RADIUS サーバに送られます。これはユーザをさまざまなグループに分類するために使用されます。最大 32 文字の英数字を入力できます。リリース 7.4 以降では、NAS-ID をインターフェイス、WLAN、またはアクセス ポイント グループに設定できます。優先順位は AP グループの NAS-ID > WLAN の NAS-ID > インターフェイスの NAS-ID の順です。
none	コントローラのシステム名を NAS-ID として設定します。
profile-mapping	AP グループの RF プロファイル マッピングを設定します。
profile_name	指定した AP グループの RF プロファイル名。
wlan-radio-policy	AP グループに WLAN 無線ポリシーを設定します。
802.11a-only	AP グループに WLAN 無線ポリシーを設定します。
802.11bg	AP グループに WLAN 無線ポリシーを設定します。
802.11g-only	AP グループに WLAN 無線ポリシーを設定します。
all	AP グループに WLAN 無線ポリシーを設定します。
hotspot	AP グループのホットスポットを設定します。
venue	AP グループの場所情報を設定します。
type	AP グループの場所のタイプを設定します。

group_code	AP グループの場所グループの情報。 次のオプションを使用できます。 • 0：指定なし • 1：集会施設 • 2：ビジネス • 3：教育 • 4: 工場および産業 • 5：機関 • 6：商業施設 • 7：居住施設 • 8：倉庫 • 9: 公共施設、その他 • 10：乗り物 • 11：アウトドア

type_code

AP グループの場所タイプの情報。

場所グループ 1（集会施設）には、次のオプションが使用できます。

- 0：指定されていない集会施設
- 1：アリーナ
- 2：スタジアム
- 3：旅客ターミナル
- 4：円形劇場
- 5：遊園地
- 6：礼拝場所
- 7：会議室
- 8：図書館
- 9：博物館
- 10：レストラン
- 11：シアター
- 12：バー
- 13：カフェ
- 14: 動物園または水族館
- 15：緊急時の調整センター

場所グループ 2（ビジネス）には、次のオプションが使用できます。

- 0：指定されていないビジネス
- 1：医師または歯科医のオフィス
- 2：銀行
- 3：消防局
- 4：警察署
- 6：郵便局
- 7：専門家のオフィス
- 8：研究開発施設
- 9：弁護士のオフィス

場所グループ 3（教育施設）には、次のオプションが使用できます。

- 0：指定されていない教育施設
- 1：小学校
- 2：中学校
- 3：大学または専門学校

場所グループ 4（工場および産業）には、次のオプションが使用できます。

- 0：指定されていない工場および産業
- 1：工場

場所グループ 5（機関）には、次のオプションが使用できます。

- 0：指定されていない機関
- 1：病院
- 2：長期介護施設
- 3：アルコールおよび麻薬のリハビリテーション センター
- 4: グループ ホーム
- 5:刑務所や拘置所

場所グループ 6（商業施設）には、次のオプションが使用できます。

- 0：指定されていない商業施設
- 1：小売店
- 2：食料品市場
- 3：自動車サービス ステーション
- 4：ショッピング モール
- 5：ガソリン スタンド

場所グループ 7（居住施設）には、次のオプションが使用できます。

- 0：指定されていない居住施設
- 1：個人の住宅
- 2：ホテルまたはモーテル
- 3：寮
- 4：寄宿舎

場所グループ8（倉庫）には、次のオプションが使用できます。

- 0：指定されていない倉庫

場所グループ9（公共施設、その他）には、次のオプションが使用できます。

- 0：指定されていない公共施設およびその他

場所グループ10（乗り物）には、次のオプションが使用できます。

- 0：指定されていない乗り物
- 1：自動車またはトラック
- 2：航空機
- 3：バス
- 4：フェリー
- 5：船舶またはボート
- 6：鉄道
- 7：バイク

	場所グループ 11（アウトドア）には、次のオプションが使用できます。 • 0：指定されていないアウトドア • 1: ミニメッシュ ネットワーク • 2：都市公園 • 3：休憩所 • 4：交通制御施設 • 5：バス停 • 6：キオスク
name	AP グループの場所の名前を設定します。
language_code	場所で使用される言語を定義するの ISO-639 符号化文字列。この文字列は3文字の言語コードです。たとえば、英語の場合はENGと入力します。
venue_name	このAPグループ会場の名前。この名前は、基本サービス セット（BSS）に関連付けられ、SSIDで場所に関する十分な情報が得られないときに使用されます。場所の名前は最大 252 文字の英数字で、大文字と小文字を区別します。
add	AP グループの運用クラスを追加します。
delete	AP グループの運用クラスを削除します。
operating_class_value	APグループの運用クラス。使用可能な運用クラスは、81、83、84、112、113、115、116、117、118、119、120、121、122、123、124、125、126、127 です。

コマンド デフォルト

AP グループの VLAN は無効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

1 つ以上のアクセス ポイントで使用しているアクセス ポイント グループを削除しようとすると、エラー メッセージが表示されます。コントローラ ソフトウェア リリース 6.0 で AP を削除するには、まず、このグループのすべての AP を別のグループに移動します。以前のリリースのように、アクセス ポイントが default-group アクセス ポイント グループに移動されること

はありません。AP を表示するには、**show wlan apgroups** コマンドを入力します。AP を移動するには、**config ap group-name***groupname cisco_ap* コマンドを入力します。

AP グループ、WLAN、またはインターフェイスのコントローラに設定されている NAS-ID が認証に使用されます。NAS-ID はコントローラに伝播されません。

次に、アクセス ポイント グループ 4 で、NAC アウトオブバンド サポートをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan apgroup nac enable apgroup 4
```

config wlan apgroup atf 802.11

config wlan apgroup atf 802.11 コマンドを使用して、AP グループ レベルでの Cisco Airtime Fairness を設定します。

config wlan apgroups atf 802.11{**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} *ap-group-name*} | {**optimization** {**enable** | **disable**}}

構文の説明

a	802.11a ネットワーク設定を指定します。
b	802.11b/g ネットワーク設定を指定します。
mode	Cisco ATF の強制のきめ細かさを設定します。
disable	Cisco ATF を無効にします。
monitor	Cisco ATF をモニタ モードで設定します。
enforce-policy	Cisco ATF を強制モードで設定します。
ap-group-name	指定する必要がある AP グループ名
optimization	通信時間の最適化を設定します。
enable	通信時間の最適化を有効にします。
disable	通信時間の最適化を無効にします。

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

802.11a ネットワークで Cisco ATF を強制モードで設定するには、AP グループ *my-ap-group*に、次のコマンドを入力します。

```
(Cisco Controller) >config wlan apgroup atf 802.11a mode enforce-policy my-ap-group
```

config wlan apgroup atf 802.11 policy

WLAN で Cisco ATF ポリシーの AP レベルのオーバーライドを設定するには、次のコマンドを使用します。

config wlan apgroup atf 802.11 {**a** | **b**} **policy** *ap-group-name wlan-id policy-name* **override** {**enable** | **disable**}

構文の説明

a	802.11a ネットワーク設定を指定します。
b	802.11b ネットワーク設定を指定します。
policy	Cisco ATF ポリシーを指定します。
ap-group-name	指定する必要がある AP グループ名
wlan-id	指定する必要がある WLAN ID またはリモート LAN ID。
policy-name	指定する必要がある Cisco ATF ポリシー名。
override	AP グループの WLAN の ATF ポリシー オーバーライドを設定します。
enable	AP グループの WLAN の ATF ポリシー オーバーライドを有効にします。
disable	AP グループの WLAN の ATF ポリシー オーバーライドを無効にします。

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

config wlan apgroup qinq

AP グループのトラフィックの 802.1Q-in-Q VLAN タギングを設定するには、**config wlan apgroup qinq** コマンドを使用します。

config wlan apgroup qinq {**tagging** {**client-traffic | dhcp-v4 | eap-sim-aka**} *apgroup_name* {**enable | disable**}|**service-vlan***apgroup_name vlan_id*}

構文の説明

tagging	トラフィックの 802.1Q-in-Q VLAN タギングを設定します。
client-traffic	AP グループのクライアント トラフィックの 802.1Q-in-Q タギングを設定します。
dhcp-v4	AP グループの DHCPv4 トラフィックの 802.1Q-in-Q タギングを設定します。
eap-sim-aka	AP グループの Extensible Authentication Protocol for Authentication and Key Agreement（EAP-AKA）、および EAP for Global System for Mobile Communications Subscriber Identity Module（EAP-SIM）トラフィックの 802.1Q-in-Q タギングを設定します。
enable	トラフィックの 802.1Q-in-Q タギングを有効にします。
disable	トラフィックの 802.1Q-in-Q タギングを無効にします。
service-vlan	AP グループのサービス VLAN を設定します。
apgroup_name	アクセス ポイント グループの名前。
vlan_id	VLAN 識別番号。

コマンド デフォルト

デフォルトでは、AP グループのクライアントおよび DHCPv4 トラフィックの 802.1Q-in-Q タギングは無効です。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

（注） DHCPv4 トラフィックの 802.1Q-in-Q タギングを有効にする前に、クライアント トラフィックの 802.1Q-in-Q タギングを有効にする必要があります。

クライアント トラフィックの 802.1Q-in-Q タギングを有効にすると、EAP-AKA および EAP-SIM トラフィックの 802.1Q-in-Q タギング も有効になります。

次に、AP グループのクライアント トラフィックの 802.1Q-in-Q タギングを有効にする例を示します。

```
(Cisco Controller) >config wlan apgroup qinq tagging client-traffic APg1 enable
```

次に、AP グループのサービス VLAN を設定する例を示します。

```
(Cisco Controller) >config wlan apgroup qinq service-vlan APg1 10
```

config wlan assisted-roaming

WLAN で経由ローミングを設定するには、**config wlan assisted-roaming** コマンドを使用します。

config wlan assisted-roaming {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

構文の説明

neighbor-list	WLAN の 802.11k ネイバー リストを設定します。
dual-list	WLAN のデュアル バンド 802.11k ネイバー リストを設定します。デフォルトは、クライアントが現在関連付けられている帯域です。
prediction	WLAN の経由ローミング最適化の予測を設定します。
enable	WLAN の設定をイネーブルにします。
disable	WLAN の設定をディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

すべての WLAN で 802.11k ネイバー リストが有効です。

デフォルトでは、ネイバー リスト機能が WLAN に対してイネーブルな場合に、デュアル バンド リストはイネーブルになります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

経由ローミングの予測のリストをイネーブルにすると、警告が表示されます。また、WLAN でロードバランシングがすでにイネーブルになっている場合、ロードバランシングはその WLAN でディセーブルになります。

次に、WLAN の 802.11k ネイバー リストをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

config wlan atf

config wlan atf コマンドを使用して、Cisco ATF ポリシーに WLAN をマッピングします。

config wlan atf *wlan-id* **policy** *policy-id*

構文の説明

wlan-id	Cisco ATF ポリシーをマッピングする必要がある、指定すべき WLAN ID。
policy	Cisco ATF ポリシーを指定します。
policy-id	指定する必要がある Cisco ATF ポリシー ID。

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

config wlan avc

WLAN に Application Visibility and Control（AVC）を設定するには、**config wlan avc** コマンドを使用します。

config wlan avc *wlan_id* {**profile** *profile_name* | **visibility**} {**enable** | **disable**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
profile	WLAN から AVC プロファイルをアソシエーションまたは削除します。
profile_name	AVC プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。
visibility	WLAN にアプリケーションの表示を設定します。
enable	WLAN でアプリケーションの表示をイネーブルにします。Network Based Application Recognition（NBAR）ディープ パケット インスペクション テクノロジーに基づいて、アプリケーションの分類を確認できます。 クライアント AVC 統計情報を表示するには、**show avc statistics client** コマンドを使用します。
disable	WLAN でアプリケーションの表示をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

1 つの WLAN には AVC プロファイルを 1 つだけ設定できます。また各 AVC プロファイルに最大 32 のルールを設定できます。各ルールはアプリケーションに対してマーキングまたは廃棄アクションを指定し、WLAN ごとに最大 32 のアプリケーションのアクションを設定できます。コントローラ 1 台に最大 16 の AVC プロファイルを設定し、AVC プロファイル 1 つを複数の WLAN に関連付けることができます。

次に、WLAN に AVC プロファイルを関連付ける例を示します。

```
(Cisco Controller) >config wlan avc 5 profile profile1 enable
```

config wlan band-select allow

WLAN で帯域選択を設定するには、**config wlan band-select allow** コマンドを使用します。

config wlan band-select allow {**enable** | **disable**} *wlan_id*

構文の説明

enable	WLAN で帯域選択をイネーブルにします。
disable	WLANで帯域選択をディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

WLAN で帯域選択を有効にすると、アクセス ポイントによって 2.4 GHz でのクライアント プローブが抑制され、デュアル バンド クライアントが 5 Ghz スペクトルに移動されます。帯域選択アルゴリズムによるデュアルバンドクライアントの誘導は、同じアクセスポイントの2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。

次に、WLAN で帯域選択をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan band-select allow enable 6
```

config wlan broadcast-ssid

無線 LAN でサービス セット識別子（SSID）ブロードキャストを設定するには、**config wlan broadcast-ssid** コマンドを使用します。

config wlan broadcast-ssid {**enable** | **disable**} *wlan_id*

構文の説明

enable	無線 LAN で SSID ブロードキャストをイネーブルにします。
disable	無線LANでSSIDブロードキャストをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

SSID のブロードキャストはディセーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、無線 LAN ID 1 の SSID ブロードキャストを設定する例を示します。

```
(Cisco Controller) >config wlan broadcast-ssid enable 1
```

config wlan call-snoop

特定の WLAN に対して Voice-over-IP（VoIP）スヌーピングをイネーブルまたはディセーブルにするには、**config wlan call-snoop** コマンドを使用します。

config wlan call-snoop {**enable** | **disable**} *wlan_id*

構文の説明

enable	無線 LAN 上の VoIP スヌーピングをイネーブルにします。
disable	無線 LAN 上の VoIP スヌーピングをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

WLAN は Platinum QoS とし、この CLI を起動中にディセーブルにする必要があります。

次の例では、VoIP スヌーピングを WLAN 3 でイネーブルにする方法を示します。

```
(Cisco Controller) >config wlan call-snoop 3 enable
```

config wlan chd

無線 LAN に対してカバレッジ ホール検出（CHD）を有効または無効にするには、**config wlan chd** コマンドを使用します。

config wlan chd *wlan_id* {**enable** | **disable**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
enable	無線 LAN で SSID ブロードキャストをイネーブルにします。
disable	無線 LAN で SSID ブロードキャストをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次の例では、CHD を WLAN 3 でイネーブルにする方法を示します。

```
(Cisco Controller) >config wlan chd 3 enable
```

config wlan ccx aironet-ie

WLAN に対する Aironet 情報要素（IE）を有効または無効にするには、**config wlan ccx aironet-ie** コマンドを使用します。

config wlan ccx aironet-ie {**enable** | **disable**}

構文の説明

enable	Aironet 情報要素をイネーブルにします。
disable	Aironet 情報要素をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN に対する Aironet 情報要素をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan ccx aironet-ie enable
```

config wlan channel-scan defer-priority

オフ チャネル スキャンを延期できるパケットの優先順位マーキングに対して、延期するようにコントローラを設定するには、**config wlan channel-scan defer-priority** コマンドを使用します。

config wlan channel-scan defer-priority *priority* ［**enable** | **disable**］ *wlan_id*

構文の説明

priority	ユーザ プライオリティ値（0～7）。
enable	（任意）特定の優先順位のパケットでオフチャネル スキャンの延期をイネーブルにします。
disable	（任意）特定の優先順位のパケットでオフチャネルスキャンの延期をディセーブルにします。
wlan_id	無線 LAN 識別子（1～512）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

priority 値は、クライアントおよび WLAN では 6 に設定する必要があります。

次に、ユーザ プライオリティ値 6 および WLAN ID 30 のオフ チャネル スキャンを延期できる優先順位マーキングのコントローラによる延期をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan channel-scan defer-priority 6 enable 30
```

config wlan channel-scan defer-time

ミリ秒単位でチャネル スキャンの遅延時間を割り当てるには、**config wlan channel-scan defer-time** コマンドを使用します。

config wlan channel-scan defer-time *msecs wlan_id*

構文の説明

msecs	ミリ秒単位の遅延時間（0～60000 ミリ秒）。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ミリ秒単位の時間値は、WLAN 機器の要件を満たす必要があります。

次に、WLAN ID 50 に対して、40 ミリ秒のスキャン遅延時間を割り当てる例を示します。

```
(Cisco Controller) >config wlan channel-scan defer-time 40 50
```

config wlan custom-web

WLAN の Web 認証ページを設定するには、**config wlan custom-web** コマンドを使用します。

config wlan custom-web{ {**ext-webauth-url** *ext-webauth-url wlan_id* } | {**global** {**enable** | **disable**}} | {**ms-open** {**enable** | **disable** |**url**}} | {**login-page** *page-name* } | {**loginfailure-page** {*page-name* | **none**}} | {**logout-page** {*page-name* | **none**}} | {**sleep-client** {**enable** | **disable**} *wlan_id* **timeout** *duration*} | {**webauth-type** {**internal** | **customized** | **external**} *wlan_id*}}

構文の説明

ext-webauth-url	外部 Web 認証の URL を設定します。
ext-webauth-url	外部 Web 認証の URL。
wlan_id	WLAN 識別子。デフォルトの範囲は 1 ～ 512 です。
global	WLAN のグローバル ステータスを設定します。
enable	WLAN のグローバル ステータスをイネーブルにします。
disable	WLAN のグローバル ステータスをディセーブルにします。
ms-open	WLAN で ms オープン機能を設定します。
enable	WLAN で ms オープン機能をイネーブルにします。
disable	WLAN で ms オープン機能をディセーブルにします。
url	ms オープン URL を設定します。
login-page	外部 Web 認証 URL へのログイン ページの名前を設定します。
page-name	外部 Web 認証 URL へのログイン ページ名。
loginfailure-page	外部 Web 認証 URL へのログイン失敗ページの名前を設定します。
none	外部 Web 認証 URL へのログイン失敗ページを設定しません。
logout-page	外部 Web 認証 URL のログアウト ページの名前を設定します。
sleep-client	WLAN でスリープ クライアント機能を設定します。
timeout	WLAN でスリープ クライアントのタイムアウトを設定します。

duration	スリープ状態にあるクライアントが強制的に再認証されるまでの、アイドル タイムアウト後の最大時間数（時間単位）。範囲は 1 ～ 720 時間です。デフォルト値は 12 です。スリープ クライアント機能が有効になると、スリープと再起動時間の間、クライアントは同じモビリティ グループ内で 1 つの Cisco WLC から別の Cisco WLC に移動した場合、ログイン資格情報を入力する必要はありません。
webauth-type	WLAN 用の Web 認証のタイプを設定します。
internal	デフォルト ログイン ページを表示します。
customized	カスタマイズされたログイン ページを表示します。
external	外部 Web サーバにあるログイン ページを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.2	このコマンドが変更され、ms オープン パラメータが追加されました。

次に、WLAN で Web 認証タイプを設定する例を示します。

```
Cisco Controller config wlan custom-web webauth-type external
```

config wlan dhcp_server

無線 LAN の内部 DHCP サーバを設定するには、**config wlan dhcp_server** コマンドを使用します。

config wlan dhcp_server {*wlan_id* | **foreignAp**} *ip_address* [**required**]

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
ip_address	内部 DHCP サーバの IP アドレス（このパラメータは必須です）。
required	（任意）DHCP アドレス割り当てが必要かどうかを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

DHCP の設定には、DHCP サーバのオーバーライドではなく、特定のインターフェイスに割り当てられたプライマリの DHCP アドレスを使用する方式が優先されます。オーバーライドを有効にする場合は、**show wlan** コマンドを使用して、DHCP サーバが WLAN に割り当てられていることを確認できます。

次に、無線 LAN ID 16 の内部 DHCP サーバの IP アドレス 10.10.2.1 を設定する例を示します。

```
(Cisco Controller) >config wlan dhcp_server 16 10.10.2.1
```

config wlan diag-channel

特定の WLAN で診断チャネルのトラブルシューティングを有効にするには、**config wlan diag-channel** コマンドを使用します。

config wlan diag-channel ［**enable** | **disable**］ *wlan_id*

構文の説明

enable	（任意）無線LANの診断チャネルをイネーブルにします。
disable	（任意）無線LANの診断チャネルをディセーブルにします。
wlan_id	無線 LAN 識別子（1～512）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 1 の無線 LAN の診断チャネルをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan diag-channel enable 1
```

config wlan dtim

802.11 無線ネットワークの Delivery Traffic Indicator Message（DTIM）を設定するには、**config wlan dtim** コマンドを使用します。

config wlan dtim {**802.11a** | **802.11b**} *dtim wlan_id*

構文の説明

802.11a	802.11a 無線ネットワークの DTIM を設定します。
802.11b	802.11b 無線ネットワークの DTIM を設定します。
dtim	DTIM の値（1 ～ 255）。
wlan_id	設定する WLAN の番号。

コマンド デフォルト

デフォルトは DTIM 1 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、DTIM 値 128 および WLAN ID 1 で、802.11a 無線ネットワークの DTIM を設定する例を示します。

```
(Cisco Controller) >config wlan dtim 802.11a 128 1
```

config wlan exclusionlist

無線 LAN の除外リストを設定するには、**config wlan exclusionlist** コマンドを使用します。

config wlan exclusionlist {*wlan_id* [**enabled** | **disabled** | *time*] | **foreignAp** [**enabled** | **disabled** | *time*]}

構文の説明

wlan_id	無線 LAN 識別子（1～512）。
enabled	（任意）特定の無線LANまたは外部アクセスポイントの除外リストをイネーブルにします。
disabled	（任意）特定の無線LANまたは外部アクセスポイントの除外リストをディセーブルにします。
time	（任意）除外リスト タイムアウト（秒）。値 0 は無期限を示します。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは **config wlan blacklist** コマンドの代わりに使用します。

次に、WLAN ID 1 の除外リストをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan exclusionlist 1 enabled
```

config wlan fabric

WLAN でファブリックを有効または無効にするには、**config wlan fabric** コマンドを使用します。

config wlan fabric {**enable** | **disable**} *wlan-id*

構文の説明

enable	WLAN でファブリックをイネーブルにします。
disable	WLANでファブリックをディセーブルにします。
wlan-id	WLAN 識別子。

コマンド デフォルト

コマンド モード

コマンド履歴

リリース	変更内容
8.5	このコマンドが導入されました。

使用上のガイドライン

非ファブリック AP はファブリック WLAN では設定されません。

例

次に、WLAN でファブリックをイネーブルにする例を示します。

```
config wlan fabric enable wlan1
```

config wlan flexconnect ap-auth

ローカルでスイッチされる WLAN で、FlexConnect に関連付けられるクライアントのローカル認証を設定するには、**config wlan flexconnect ap-auth** コマンドを使用します。

config wlan flexconnect ap-auth *wlan_id* {**enable** | **disable**}

構文の説明

ap-auth	ローカルでスイッチされる WLAN で、FlexConnect に関連付けられたクライアントのローカル認証を設定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
enable	WLAN の AP 認証をイネーブルにします。
disable	WLAN の AP 認証をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

FlexConnect に関連付けられたクライアントのローカル認証を設定する WLAN で、ローカル スイッチングをイネーブルにする必要があります。

次に、指定した WLAN で FlexConnect に関連付けられているクライアントの認証をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect ap-auth 6 enable
```

config wlan flexconnect central-assoc

Cisco WLC でクライアントの再アソシエーションとセキュリティ キーのキャッシュを設定するには、**config wlan flexconnect central-assoc** コマンドを使用します。

config wlan flexconnect central-assoc *wlan-id* {**enable** | **disable**}

構文の説明

wlan-id	WLAN の ID
enable	Cisco WLC のクライアントの再アソシエーションとセキュリティ キーのキャッシュを有効にします。
disable	Cisco WLC のクライアントの再アソシエーションとセキュリティ キーのキャッシュを無効にします。

コマンド デフォルト

Cisco WLC のクライアント再アソシエーションとセキュリティ キー キャッシュは、無効の状態です。

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

この設定の使用例は、高速ローミングを使用した大規模な展開です。

ローカル認証での中央アソシエーションの設定は、WLAN でサポートされません。PMIPv6 トンネルが設定されると、PMIPv6 クライアントからのすべてのデータ トラフィックは、Cisco AP から Generic Routing Encapsulation（GRE）トンネルのローカル モビリティ アンカー（LM）に転送されます。Cisco AP と Cisco WLC の間の接続が失われた場合、既存の PMIPv6 クライアントのデータ トラフィックは、Cisco AP とクライアントの間の接続が失われるまで引き続き送受信されます。AP がスタンドアロン モードの場合、PMIPv6 対応 WLAN では新規クライアント アソシエーションが受け入れられません。

次に、ID が 2 の WLAN で Cisco WLC のクライアントの再アソシエーションとセキュリティ キーのキャッシングを有効にする例を示します。

```
(Cisco Controller) >config wlan flexconnect central-assoc 2 enable
```

config wlan flexconnect learn-ipaddr

Cisco WLAN コントローラに対してクライアント IP アドレスの学習を有効または無効にするには、**config wlan flexconnect learn-ipaddr** コマンドを使用します。

config wlan flexconnect learn-ipaddr *wlan_id* {**enable** | **disable**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
enable	無線 LAN でクライアント IPv4 アドレスの学習をイネーブルにします。
disable	無線 LAN でクライアント IPv4 アドレスの学習をディセーブルにします。

コマンド デフォルト

config wlan flexconnect local-switching コマンドが無効である場合は、無効になります。**config wlan flexconnect local-switching** コマンドが有効である場合は、有効になります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

使用上のガイドライン

クライアントに Layer 2 暗号化が設定されている場合、コントローラはクライアント IP アドレスを学習できず、定期的にクライアントをドロップします。クライアント IP アドレスの学習を待たずにクライアントの接続を維持するには、このオプションを無効にします。

（注） このコマンドは IPv4 でのみ有効です。

（注） IP アドレスの学習を無効にする機能は、FlexConnect 中央スイッチングではサポートされていません。

次に、WLAN 6 に対してクライアント IP アドレスの学習をディセーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect learn-ipaddr disable 6
```

関連コマンド

show wlan

config wlan flexconnect local-switching

FlexConnect WLAN で、ローカル スイッチング、集中管理 DHCP、NAT-PAT、またはオーバーライド DNS オプションを設定するには、**config wlan flexconnect local switching** コマンドを使用します。

config wlan flexconnect local-switching *wlan_id* {**enable** | **disable**} { {**central-dhcp** {**enable** | **disable**} **nat-pat** {**enable** | **disable**} } | {**override option dns** { **enable** | **disable**} } }

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
enable	FlexConnect WLAN でローカル スイッチングをイネーブルにします。
disable	FlexConnect WLAN でローカル スイッチングをディセーブルにします。
central-dhcp	ローカル スイッチング FlexConnect WLAN で、DHCP パケットの中央スイッチングを設定します。この機能をイネーブルにすると、APから受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。
enable	FlexConnect WLAN の集中管理 DHCP をイネーブルにします。
disable	FlexConnect WLAN の集中管理 DHCP をディセーブルにします。
nat-pat	ローカル スイッチング FlexConnect WLAN で、ネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）を設定します。
enable	FlexConnect WLAN の NAT-PAT をイネーブルにします。
disable	FlexConnect WLAN の NAT-PAT をディセーブルにします。
override	FlexConnect WLAN で DHCP オーバーライド オプションを指定します。

option dns	FlexConnect WLAN でオーバーライド DNS オプションを指定します。このオプションをオーバーライドすると、クライアントは、コントローラではなく、AP から DNS サーバの IP アドレスを取得します。
enable	FlexConnect WLAN でオーバーライド DNS オプションをイネーブルにします。
disable	FlexConnect WLAN でオーバーライド DNS オプションをディセーブルにします。

コマンド デフォルト

この機能はディセーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

使用上のガイドライン

config wlan flexconnect local-switching コマンドを有効にすると、**config wlan flexconnect learn-ipaddr** コマンドもデフォルトで有効にされます。

（注） このコマンドは IPv4 でのみ有効です。

（注） IP アドレスの学習を無効にする機能は、FlexConnect 中央スイッチングではサポートされていません。

次に、ローカル スイッチングで WLAN 6 をイネーブルにし、集中管理 DHCP および NAT-PAT をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect local-switching 6 enable central-dhcp enable
 nat-pat enable
```

次に、WLAN 6 で、オーバーライド DNS オプションをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect local-switching 6 override option dns enable
```

config wlan flexconnect vlan-central-switching

ローカルでスイッチされるWLANで、中央スイッチングを設定するには、**config wlan flexconnect vlan-central-switching** コマンドを使用します。

config wlan flexconnect vlan-central-switching *wlan_id* { **enable** | **disable** }

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
enable	ローカルでスイッチされるワイヤレス LAN で、中央スイッチングをイネーブルにします。
disable	ローカルでスイッチされるワイヤレス LAN で、中央スイッチングをディセーブルにします。

コマンド デフォルト

中央スイッチングは無効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

VLAN の中央スイッチングをイネーブルにするには、Flexconnect のローカル スイッチングをイネーブルにする必要があります。WLAN 中央スイッチングをイネーブルにすると、WLAN がローカル IEEE 802.1Q リンク上で設定されている場合、アクセス ポイントはトラフィックをローカルにブリッジします。アクセス ポイントに VLAN が設定されていない場合、AP は、トンネルを使用してコントローラーにトラフィックを戻し、コントローラは対応する VLAN にトラフィックをブリッジします。

WLAN 中央スイッチングは、以下をサポートしていません。

- FlexConnect ローカル認証。
- ローカル スイッチング クライアントのレイヤ 3 ローミング。

次に、WLAN 6 で中央スイッチングをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect vlan-central-switching 6 enable
```

config wlan flow

WLAN に NetFlow モニタを関連付けるには、**config wlan flow** コマンドを使用します。

config wlan flow *wlan_id* **monitor** *monitor_name* {**enable** | **disable**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子（両端の値を含む）。
monitor	NetFlow モニタを設定します。
monitor_name	NetFlow モニタの名前。モニタ名は最大 32 文字の英数字で、大文字と小文字を区別します。モニタ名にスペースを含めることはできません。
enable	WLAN と NetFlow モニタを関連付けます。
disable	WLAN から NetFlow モニタの関連付けを解除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

config flow コマンドを使用して、新しい NetFlow モニタを作成できます。

次に、WLAN と NetFlow モニタを関連付ける例を示します。

```
(Cisco Controller) >config wlan flow 5 monitor monitor1 enable
```

config wlan hotspot

WLAN のホットスポットを設定するには、**config wlan hotspot** コマンドを使用します。

config wlan hotspot {**clear-all** *wlan_id* | **dot11u** | **hs2** | **msap**}

構文の説明

clear-all	WLAN のホットスポット設定をクリアします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
dot11u	WLAN の 802.11u ホットスポットを設定します。
hs2	WLAN の HotSpot2 を設定します。
msap	WLAN の Mobility Services Advertisement Protocol（MSAP）を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

最大 32 ホットスポット WLAN を設定できます。

次に、WLAN に HotSpot2 を設定する例を示します。

```
(Cisco Controller) >config wlan hotspot hs2 enable 2
```

config wlan hotspot dot11u

WLAN の 802.11u ホットスポットを設定するには、**config wlan hotspot dot11u** コマンドを使用します。

config wlan hotspot dot11u {**3gpp-info** | **auth-type** | **enable** | **disable** | **domain** | **hessid** | **ipaddr-type** | **nai-realm** | **network-type** | **roam-oi**}

構文の説明

3gpp-info	3GPP セルラー ネットワーク情報を設定します。
auth-type	ネットワーク認証タイプを設定します。
disable	ホットスポットのプロファイルで、802.11u をディセーブルにします。
domain	ドメインを設定します。
enable	ホットスポットのプロファイルで、802.11u をイネーブルにします。IEEE 802.11uは、モバイルまたはローミング パートナーのホットスポットで、802.1X デバイスの自動 WLAN オフロードをイネーブルにします。
hessid	Homogenous Extended Service Set Identifier（HESSID）を設定します。HESSID は、ネットワークを一意に識別する 6 オクテットの MAC アドレスです。
ipaddr-type	IPv4 アドレスの可用性タイプを設定します。
nai-realm	802.11u 対応 WLAN のレルムを設定します。
network-type	802.11u ネットワーク タイプおよびインターネット アクセスを設定します。
roam-oi	ローミング コンソーシアムの組織識別子（OI）のリストを設定します。

コマンド デフォルト

なし。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

次に、ホットスポット プロファイルで 802.11u をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

config wlan hotspot dot11u 3gpp-info

802.11u ホットスポット WLAN で 3GPP セルラー ネットワーク情報を設定するには、**config wlan hotspot dot11u 3gpp-info** コマンドを使用します。

config wlan hotspot dot11u 3gpp-info {**add** | **delete**} *index country_code network_code wlan_id*

構文の説明

add	モバイル セルラー ネットワーク情報を追加します。
delete	モバイル セルラー ネットワーク情報を削除します。
index	セルラー インデックス。指定できる範囲は 1 ～ 32 です。
country_code	2 進化 10 進数（BCD）形式のモバイル国番号（MCC）。国番号は最大 3 文字です。たとえば、米国の MCC は 310 です。
network_code	BCD形式のモバイルネットワーク コード（MNC）。モバイル国番号（MCC）と組み合わせて、MNC は携帯電話の運営事業者または通信事業者を一意に識別するために使用されます。ネットワーク コードは最大 3 文字です。たとえば、T- Mobile の MNC は 026 です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

サポートされているモバイル ネットワーク コードの数は、WLAN あたり 32 です。

次に、WLAN の 3GPP セルラー ネットワーク情報を設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u 3gpp-info add
```

config wlan hotspot dot11u auth-type

802.11u ホットスポット WLAN のネットワーク認証タイプを設定するには、**config wlan hotspot dot11u auth-type** コマンドを使用します。

config wlan hotspot dot11u auth-type *network-auth wlan_id*

構文の説明

network-auth	WLAN で設定するネットワーク認証。使用できる値は、次のとおりです。 • 0：条件に同意。 • 1：オンライン登録。 • 2：HTTP/HTTPS リダイレクション。 • 3：DNS リダイレクション。 • 4：適用されない
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

DNS リダイレクション オプションは、リリース 7.3 ではサポートされていません。

次に 802.11u ホットスポット WLAN のネットワーク認証タイプとして、HTTP/HTTPS リダイレクションを設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u auth-type 2 1
```

config wlan hotspot dot11u disable

WLAN の 802.11u ホットスポットをディセーブルにするには、**config wlan hotspot dot11u disable** コマンドを使用します。

config wlan hotspot dot11u disable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN の 802.11u ホットスポットをディセーブルにする例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u disable 6
```

config wlan hotspot dot11u domain

802.11 アクセス ネットワークで動作しているドメインを設定するには、**config wlan hotspot dot11u domain** コマンドを使用します。

config wlan hotspot dot11u domain {**add** *wlan_id domain-index domain_name* | **delete** *wlan_id domain-index* | **modify** *wlan_id domain-index domain_name*}

構文の説明

add	ドメインを追加します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
domain-index	1～32 のドメイン インデックス。
domain_name	ドメイン名。ドメイン名は最大255 文字の英数字で、大文字と小文字を区別します。
delete	ドメインを削除します。
modify	ドメインを変更します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11 アクセス ネットワークでドメインを追加する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u domain add 6 30 domain1
```

config wlan hotspot dot11u enable

WLAN の 802.11u ホットスポットをイネーブルにするには、**config wlan hotspot dot11u enable** コマンドを使用します。

config wlan hotspot dot11u enable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN の 802.11u ホットスポットをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

config wlan hotspot dot11u hessid

802.11u ホットスポット WLAN で Homogenous Extended Service Set Identifier（HESSID）を設定するには、**config wlan hotspot dot11u hessid** コマンドを使用します。

config wlan hotspot dot11u hessid *hessid wlan_id*

構文の説明

hessid	HESSID として設定できる MAC アドレス。HESSID は、ネットワークを一意に識別する 6 オクテットの MAC アドレスです。たとえば、WLAN の Basic Service Set Identification（BSSID）は、HESSID として使用できます。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に 802.11u ホットスポット WLAN の HESSID を設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u hessid 00:21:1b:ea:36:60 6
```

config wlan hotspot dot11u ipaddr-type

802.11u ホットスポット WLAN で利用できる IP アドレスのタイプを設定するには、**config wlan hotspot dot11u ipaddr-type** コマンドを使用します。

config wlan hotspot dot11u ipaddr-type *IPv4Type* {*0 - 7*} *IPv6Type* {*0 - 2*}*wlan_id*

構文の説明

IPv4Type	IPv4 タイプのアドレス。次のいずれかの値を入力します。 0：IPv4 アドレスは使用できません。 1：パブリック IPv4 アドレスが使用できます。 2：ポート制限付き IPv4 アドレスが使用できます。 3：シングル NAT 対応プライベート IPv4 アドレスが使用できます。 4：ダブル NAT 対応プライベート IPv4 アドレスが使用できます。 5：ポート制限付き IPv4 アドレスおよびシングル NAT 対応 IPv4 アドレスが使用できます。 6：ポート制限付き IPv4 アドレスおよびダブル NAT 対応 IPv4 アドレスが使用できます。 7：IPv4 アドレスが使用できるかどうかが不明です。
IPv6Type	IPv6 タイプのアドレス。次のいずれかの値を入力します。 0：IPv6 アドレスは使用できません。 1：IPv6 アドレスは使用できます。 2：IPv6 アドレスが使用できるかどうかが不明です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

IPv4 タイプのアドレスのデフォルト値は 1 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

次に 802.11u ホットスポット WLAN の IP アドレスの可用性タイプを設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u ipaddr-type 6 2 6
```

関連コマンド

show wlan

config wlan hotspot dot11u nai-realm

WLANの802.11uホットスポットのレルムを設定するには、**config wlan hotspot dot11u nai-realm** コマンドを使用します。

config wlan hotspot dot11u nai-realm {**add** | **delete** | **modify**} {**auth-method** *wlan_id realm-index eap-index auth-index auth-method auth-parameter* | **eap-method** *wlan_id realm-index eap-index eap-method* | **realm-name** *wlan_id realm-index realm*}

構文の説明

add	レルムを追加します。
delete	レルムを削除します。
modify	レルムを変更します。
auth-method	使用する認証方式を指定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
realm-index	レルム インデックス。指定できる範囲は 1 ～ 32 です。
eap-index	EAP インデックス。指定できる範囲は 1 ～ 4 です。
auth-index	認証インデックス値。値の範囲は 1 ～ 10 です。
auth-method	使用する認証方式。指定できる範囲は1 ～ 4 です。次のオプションを使用できます。 • 1：非 EAP 内部認証方式 • 2：内部認証タイプ • 3：クレデンシャル タイプ • 4：トンネル EAP 方式のクレデンシャル タイプ
auth-parameter	使用する認証パラメータ。この値は、使用する認証方式によって異なります。詳細については、次の表を参照してください。
eap-method	使用される拡張認証プロトコル（EAP）方式を指定します。

eap-method	EAP 方式。有効な範囲は 0 ～ 7 です。次のオプションを使用できます。 • 0：適用されない • 1：Lightweight Extensible Authentication Protocol（LEAP） • 2：Protected EAP（PEAP） • 3：EAP-Transport Layer Security（EAP-TLS） • 4：EAP-FAST（セキュア トンネリングを介したフレキシブル認証） • 5：EAP for GSM Subscriber Identity Module（EAP-SIM） • 6：EAP-Tunneled Transport Layer Security（EAP-TTLS） • 7：EAP for UMTS Authentication and Key Agreement（EAP-AKA）
realm-name	レルムの名前を指定します。
realm	レルムの名前。レルム名は、RFC 4282 に準拠している必要があります。たとえば、Cisco のようになります。レルム名は最大 255 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

次の表は、認証パラメータがリストされています。

表 *10* : 認証パラメータ

非 **EAP** 内部方式（**1**）	内部 **EAP** 認証方式のタイプ（**2**）	クレデンシャル タイプ（**3**）**/Tunneled EAP** クレデンシャル タイプ（**4**）
0：予約済 1：Password Authentication Protocol（PAP） 2：Challenge-Handshake Authentication Protocol（CHAP） 3：Microsoft Challenge Handshake Authentication Protocol（MS-CHAP） 4：MSCHAPV2	1：LEAP 2：PEAP 3：EAP-TLS 4：EAP-FAST 5：EAP-SIM 6：EAP-TTLS 7：EAP-AKA	1：SIM 2：USIM 3：NFC セキュア エレメント 4：ハードウェア トークン 5：ソフト トークン 6：証明書 7：ユーザ名/パスワード 8：Reserver 9：匿名 10：ベンダー固有

次に、WLAN 4 で Tunneled EAP Method Credential 認証方式を追加する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add auth-method 4 10 3 5 4 6
```

config wlan hotspot dot11u network-type

802.11u ホットスポット WLAN のネットワーク タイプとインターネットの可用性を設定するには、**config wlan hotspot dot11u network-type** コマンドを使用します。

config wlan hotspot dot11u network-type *wlan_id network-type internet-access*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
network-type	ネットワーク タイプ。使用できるオプションは、次のとおりです。 • 0：プライベート ネットワーク • 1：ゲスト アクセスを使用したプライベート ネットワーク • 2：有料のパブリック ネットワーク • 3：無料のパブリック ネットワーク • 4：個人のデバイス ネットワーク • 5：緊急サービス専用ネットワーク • 14：テストまたは実験用 • 15：ワイルドカード
internet-access	インターネット可用性のステータス。0 の値は、インターネットを使用できないこと、1 はインターネットを使用できることを示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に 802.11u ホットスポット WLAN でネットワーク タイプとインターネットの可用性を設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u network-type 2 1
```

config wlan hotspot dot11u roam-oi

802.11u ホットスポット WLAN でローミング コンソーシアムの組織識別子（OI）のリストを設定するには、**config wlan hotspot dot11u roam-oi** コマンドを使用します。

config wlan hotspot dot11u roam-oi {**add** *wlan_id oi-index oi is-beacon* | **modify** *wlan_id oi-index oi is-beacon* | **delete** *wlan_id oi-index*}

構文の説明

add	OI を追加します。
wlan-id	1 ～ 512 の無線 LAN 識別子。
oi-index	1～32 の範囲のインデックス。
oi	有効な 6 桁の 16 進数、長さを 6 バイトにする必要がある番号。たとえば、004096 または AABBDF とします。
is-beacon	ビーコンに OI を追加するために使用するビーコン フラグ。0 はディセーブル、1 がイネーブルであることを示します。フラグが設定された WLAN に対して、最大 3 つの OI を追加できます。
modify	OI を変更します。
delete	OI を削除します。

コマンド デフォルト

なし。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ローミング コンソーシアムの OI リストを設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u roam-oi add 4 10 004096 1
```

config wlan hotspot hs2

HotSpot2 パラメータを設定するには、**config wlan hotspot hs2** コマンドを使用します。

config wlan hotspot hs2 {**disable** *wlan_id* | **enable** *wlan_id* | **operator-name** {**add** *wlan_id index operator_name language-code* | **delete** *wlan_id index* | **modify** *wlan_id index operator-name language-code*} | **port-config** {**add** *wlan_id port_config_index ip-protocol port-number status* | **delete** *wlan_id port-config-index* | **modify** *wlan_id port-config-index ip-protocol port-number status*} | **wan-metrics** *wlan_id link-status symet-link downlink-speed uplink-speed* }

構文の説明

disable	HotSpot2 をディセーブルにします。
wlan-id	1 ～ 512 の無線 LAN 識別子。
enable	HotSpot2 をイネーブルにします。
operator-name	802.11 オペレータの名前を指定します。
add	WLAN 設定に、オペレータ名、ポート設定、または WAN メトリック パラメータを追加します。
index	オペレータのインデックス。指定できる範囲は 1 ～ 32 です。
operator-name	オペレータの名前。
language-code	使用する言語。言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。言語の最初の 3 文字を英語で入力します（たとえば、英語の場合はeng）。
delete	WLAN からオペレータ名、ポート設定、またはWANメトリック パラメータを削除します。
modify	WLAN のオペレータ名、ポート設定、または WAN メトリック パラメータを変更します。
port-config	ポート設定値を設定します。
port_config_index	ポート設定インデックス。指定できる範囲は 1 ～ 32 です。デフォルト値は 1 です。

ip-protocol	使用するプロトコル。このパラメータは、頻繁に使用される通信プロトコルとポートの接続状態に関する情報を提供します。次のオプションを使用できます。 1：ICMP 6：FTP/SSH/TLS/PPTP-VPN/VoIP 17：IKEv2（IPSec-VPN/VoIP/ESP） 50：ESP（IPSec-VPN）
port-number	ポート番号。次のオプションを使用できます。 0：ICMP/ESP（IPSec-VPN） 20：FTP 22：SSH 443：TLS-VPN 500：IKEv2 1723：PPTP-VPN 4500：IKEv2 5060：VoIP
status	IP ポートのステータス。次のオプションを使用できます。 0：クローズ 1：オープン 2：不明
wan-metrics	WAN メトリックを設定します。
link-status	リンク ステータス。次のオプションを使用できます。 • 0：不明 • 1：リンク アップ • 2：リンク ダウン • 3：テスト状態のリンク

symet-link	対称的なリンク ステータス。次のオプションを使用できます。 • 0：リンク速度はアップリンクとダウンリンクで異なります（ADSL など）。 • 1：リンク速度はアップリンクとダウンリンクで同じです（DS1 など）。
downlink-speed	kbps 単位の WAN バックホール リンクのダウンリンク速度。最大値は 4,194,304 kbps です。
uplink-speed	kbps 単位の WAN バックホール リンクのアップリンク速度。最大値は 4,194,304 kbps です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WAN メトリック パラメータの設定例を示します。

```
(Cisco Controller) >config wlan hotspot hs2 wan-metrics add 345 1 0 3333
```

config wlan hotspot hs2 domain-id

ドメイン ID を設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 domain-id** コマンドを使用します。

config wlan hotspot hs2 domain-id *wlan-id domain-id*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
domain-id	ドメイン ID。0 ～ 65535 の範囲で値を入力します。

コマンド デフォルト

ドメイン ID が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、ドメイン ID を設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 domain-id 12 2
```

config wlan hotspot hs2 osu legacy-ssid

オンライン サインアップ（OSU）サービス セット識別子（SSID）名を設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu legacy-ssid** コマンドを使用します。

config wlan hotspot hs2 osu legacy-ssid *wlan-id ssid-name*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
ssid-name	SSID 名。

コマンド デフォルト

OSU SSID 名が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU SSID 名を設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu legacy-ssid 12 cisco
```

config wlan hotspot hs2 osu sp create

オンライン サインアップ（OSU）サービス プロバイダー名を作成するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp create** コマンドを使用します。

config wlan hotspot hs2 osu sp create *wlan-id osu-index lang-code* **ascii/hex** *friendly-name* [*description*]

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。
lang-code	言語コード。ISO-639 の 2 文字または 3 文字のコードを入力します（たとえば、英語の場合は *eng*）。
ascii/hex	テキスト形式を指定します（ASCII または 16 進数）。
friendly-name	サービス プロバイダー名。最大文字数は 252 文字です。
description	（任意）サーバの説明。最大文字数は 252 文字です。

コマンド デフォルト

OSU サービス プロバイダー名が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU サービス プロバイダー名を設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp create 12 2 eng ascii cisco server-1
```

config wlan hotspot hs2 osu sp delete

オンライン サインアップ（OSU）サービス プロバイダーを削除するには、**config wlan hotspot hs2 osu sp delete**コマンドを使用します。

config wlan hotspot hs2 osu sp delete *wlan-idosu-index lang-code*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。
lang-code	言語コード。ISO-639 の 2 文字または 3 文字のコードを入力します（たとえば、英語の場合は *eng*）。

コマンド デフォルト

OSU サービス プロバイダーが設定されます。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU サービス プロバイダーを削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp delete 12 2 eng
```

config wlan hotspot hs2 osu sp icon-file add

特定の WLAN でオンライン サインアップ（OSU）アイコン ファイルを設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp icon-file add** コマンドを使用します。

config wlan hotspot hs2 osu sp icon-file add *wlan-idosu-index icon-filename*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。
icon-filename	アイコンのファイル名です。

コマンド デフォルト

OSU アイコン ファイルが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**config icon** *file-info* コマンドを使用してアイコン パラメータを設定します。

次に、WLAN で OSU アイコン ファイルを設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp icon-file add 12 2 test-icon
```

config wlan hotspot hs2 osu sp icon-file delete

WLAN からオンライン サインアップ（OSU）アイコン ファイルを削除するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp icon-file delete** コマンドを使用します。

config wlan hotspot hs2 osu sp icon-file delete *wlan-idosu-index icon-filename*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。
icon-filename	アイコンのファイル名です。

コマンド デフォルト

OSU アイコン ファイルが設定されます。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、WLAN から OSU アイコン ファイルを削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp icon-file delete 12 2 test-icon
```

config wlan hotspot hs2 osu sp method add

オンライン サインアップ（OSU）方法リストを設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp method add** コマンドを使用します。

config wlan hotspot hs2 osu sp method add *wlan-id osu-index method-primary method-secondary*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。
method-primary	プライマリ OSU エンコード方法。有効な値は、**oma-dm** または **soap-xml** です。
method-secondary	（オプション）セカンダリ OSU エンコード方法。有効な値は、**oma-dm** または **soap-xml** です。

コマンド デフォルト

OSU 方法リストが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU 方法リストを設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp method add 12 2 oma-dm oma-dm
```

config wlan hotspot hs2 osu sp method delete

オンライン サインアップ（OSU）方法リストを削除するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp method delete** コマンドを使用します。

config wlan hotspot hs2 osu sp method delete *wlan-id osu-index method*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。
method	OSU エンコード方法。有効な値は、**oma dm** または **soap xml** です。

コマンド デフォルト

OSU 方法リストが設定されます。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU 方法リストを削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp method delete 12 2 oma-dm
```

config wlan hotspot hs2 osu sp nai add

オンライン サインアップ（OSU）ネットワーク アクセス識別子（NAI）を作成するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp nai add** コマンドを使用します。

config wlan hotspot hs2 osu sp nai add *wlan-id osu-index nai*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。
nai	OSU サーバの NAI。255 文字以内で名前を入力します。

コマンド デフォルト

OSU NAI が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU NAI を設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp nai add 12 2 nai-1
```

config wlan hotspot hs2 osu sp nai delete

オンライン サインアップ（OSU）ネットワーク アクセス識別子（NAI）を削除するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp nai delete** コマンドを使用します。

config wlan hotspot hs2 osu sp nai delete *wlan-id osu-index*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。

コマンド デフォルト

OSU NAI が設定されます。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU NAI を削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp nai delete 12 2
```

config wlan hotspot hs2 osu sp uri add

オンライン サインアップ（OSU）URI を作成するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp uri add** コマンドを使用します。

config wlan hotspot hs2 osu sp uri add *wlan-id osu-index uri*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。
uri	OSU サーバ名。最大 255 文字の Uniform Resource Identifier（URI） を入力します。

コマンド デフォルト

OSU URI が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU NAI を作成する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp uri add 12 2 server
```

config wlan hotspot hs2 osu sp uri delete

オンライン サインアップ（OSU）URI を削除するには、**config wlan hotspot hs2 osu sp uri delete** コマンドを使用します。

config wlan hotspot hs2 osu sp uri delete *wlan-idosu-index*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
osu-index	OSU インデックス。1 ～ 16 の範囲で値を入力します。

コマンド デフォルト

OSU URI が設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、OSU URI を削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp uri delete 12 2
```

config wlan hotspot hs2 wan-metrics downlink

ダウンリンク WAN メトリックを設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 wan-metrics downlink** コマンドを使用します。

config wlan hotspot hs2 wan-metrics downlink *wlan-id dlink-speed dlink-load*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
dlink-speed	kbps 単位の WAN バックホール リンクの速度。範囲は 0 ～ 4,294,967,295 です。
dlink-load	WAN バックホール リンクの負荷。範囲は 0 ～ 100 です。

コマンド デフォルト

ダウンリンク WAN メトリックが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、ダウンリンク WAN メトリックの設定例を示します。

```
Cisco Controller > config wlan hotspot hs2 wan-metrics downlink 12 2468 10
```

config wlan hotspot hs2 wan-metrics link-status

WAN メトリックのリンク ステータスを設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 wan-metrics link-status** コマンドを使用します。

config wlan hotspot hs2 wan-metrics link-status *wlan-id link-status*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
link-status	リンク ステータス。有効な値は次のとおりです。 • **0**：不明 • **1**：アップ • **2**：ダウン • **3**：テスト

コマンド デフォルト

リンク ステータスが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、WAN メトリックのリンク ステータスの設定例を示します。

```
Cisco Controller > config wlan hotspot hs2 wan-metrics link-status 12 1
```

config wlan hotspot hs2 wan-metrics lmd

WAN メトリックの負荷測定期間を設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 wan-metrics lmd** コマンドを使用します。

config wlan hotspot hs2 wan-metrics lmd *wlan-id lmd-value*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
lmd-value	WAN の負荷測定期間。範囲は 0 ～ 65535 です。

コマンド デフォルト

WAN の負荷測定期間が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、WAN メトリックの負荷測定期間の設定例を示します。

```
Cisco Controller > config wlan hotspot hs2 wan-metrics lmd 1 2456
```

config wlan hotspot hs2 wan-metrics uplink

アップリンク WAN メトリックを設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 wan-metrics uplink** コマンドを使用します。

config wlan hotspot hs2 wan-metrics uplink *wlan-id ulink-speed ulink-load*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。
ulink-speed	kbps 単位の WAN バックホール リンクの速度。範囲は 0 ～ 4,294,967,295 です。
ulink-load	WAN バックホール リンクの負荷。範囲は 0 ～ 100 です。

コマンド デフォルト

アップリンク WAN メトリックが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、アップリンク WAN メトリックの設定例を示します。

```
Cisco Controller > config wlan hotspot hs2 wan-metrics uplink 12 2468 10
```

config wlan hotspot msap

WLAN の Mobility Service Advertisement Protocol（MSAP）のパラメータを設定するには、**config wlan hotspot msap** コマンドを使用します。

config wlan hotspot msap {**enable** | **disable** | **server-id** *server_id*} *wlan_id*

構文の説明

enable	WLAN の MSAP をイネーブルにします。
disable	WLAN の MSAP をディセーブルにします。
server-id	MSAP サーバ ID を指定します。
server_id	MSAP サーバ ID。値の範囲は 1 ～ 10 です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN で MSAP をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan hotspot msap enable 4
```

config wlan interface

無線 LAN インターフェイスまたはインターフェイス グループを設定するには、**config wlan interface** コマンドを使用します。

config wlan interface {*wlan_id* | **foreignAp**} {*interface-name* | *interface-group-name*}

構文の説明

wlan_id	（任意）無線 LAN 識別子（1～512）。
foreignAp	サードパーティのアクセス ポイントを指定します。
interface-name	インターフェイス名。
interface-group-name	インターフェイス グループの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、VLAN901 という名前のインターフェイスを設定する例を示します。

```
(Cisco Controller) >config wlan interface 16 VLAN901
```

config wlan ipv6 acl

無線 LAN の IPv6 アクセス コントロール リスト（ACL）を設定するには、**config wlan ipv6 acl** コマンドを使用します。

config wlan ipv6 acl *wlan_id acl_name*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
acl_name	IPv6 ACL の名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ローカル スイッチング用の IPv6 ACL を設定する例を示します。

```
(Cisco Controller) >config wlan ipv6 acl 22 acl_sample
```

config wlan kts-cac

WLAN のボタン電話システム ベースの CAC ポリシーを設定するには、**config wlan kts-cac** コマンドを使用します。

config wlan kts-cac {**enable** | **disable**} *wlan_id*

構文の説明

enable	KTS ベースの CAC ポリシーをイネーブルにします。
disable	KTS ベースの CAC ポリシーをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

WLAN の KTS ベースの CAC ポリシーをイネーブルにするには、次の手順を実行します。

- WLAN の QoS プロファイルを Platinum に設定するには、次のコマンドを入力します。

  config wlan qos *wlan-id* **platinum**

- WLAN を無効にするには、次のコマンドを入力します。

  config wlan disable *wlan-id*

- WLAN に対する FlexConnect ローカル スイッチングをディセーブルにするには、次のコマンドを入力します。

  config wlan flexconnect local-switching *wlan-id* **disable**

次に、ID 4 の WLAN に対して、KTS ベースの CAC ポリシーをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan kts-cac enable 4
```

config wlan layer2 acl

中央でスイッチングされる WLAN でレイヤ 2 アクセス コントロール リスト（ACL）を設定するには、**config wlan acl layer2** コマンドを使用します。

config wlan layer2 acl*wlan_id* {*acl_name* | **none**}

構文の説明

wlan_id	無線 LAN の ID。範囲は 1 ～ 512 です。
acl_name	レイヤ 2 ACL 名。名前には 32 文字以内の英数字を使用できます。
none	WLAN にマッピングされた任意のレイヤ 2 ACL をクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 ACL に対して最大 16 のルールを作成できます。

Cisco WLC には、最大で 64 の レイヤ 2 ACL を作成できます。

アクセス ポイントは最大 16 の WLAN をサポートするので、アクセス ポイントごとに最大 16 のレイヤ 2 ACL がサポートされます。

アクセス ポイントはレイヤ 2 およびレイヤ 3 の同じ ACL 名をサポートしないため、レイヤ 2 ACL 名が FlexConnect ACL 名と競合していないことを確認します。

次に、WLAN にレイヤ 2 ACL を適用する例を示します。

```
(Cisco Controller) >config wlan layer2 acl 1 acl_l2_1
```

config wlan ldap

設定されている Lightweight Directory Access Protocol（LDAP）サーバへのリンクを追加または削除するには、**config wlan ldap** コマンドを入力します。

config wlan ldap {**add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*}}

構文の説明

add	設定されている LDAP サーバへのリンクを追加します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
server_id	LDAP サーバ インデックス。
delete	設定されている LDAP サーバへのリンクを削除します。
all	すべての LDAP サーバを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用して、WLAN に LDAP サーバの優先順位を指定します。

LDAP サーバの優先順位を指定するには、次のいずれかを設定し、有効にする必要があります。

- 802.1X 認証およびローカル EAP
- Web 認証および LDAP

（注） ローカル EAP はコントローラ ソフトウェア リリース 4.1 で導入されました。また、Web 認証での LDAP のサポートは、コントローラ ソフトウェア リリース 4.2 で導入されました。

次に、WLAN ID 100 およびサーバ ID 4 に設定されている LDAP サーバへのリンクを追加する例を示します。

```
(Cisco Controller) >config wlan ldap add 100 4
```

config wlan learn-ipaddr-cswlan

中央でスイッチングされる WLAN でクライアントの IP アドレス学習を設定するには、**config wlan learn-ipaddr-cswlan** コマンドを使用します。

config wlan learn-ipaddr-cswlan *wlan_id* {**enable** | **disable**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
enable	中央でスイッチングされる WLAN でのクライアントの IPv4 アドレス学習を有効にします。
disable	中央でスイッチングされる WLAN でのクライアントの IPv4 アドレス学習を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

使用上のガイドライン

クライアントに Layer 2 暗号化が設定されている場合、Cisco WLC はクライアント IP アドレスを学習できず、定期的にクライアントをドロップします。Cisco WLC がクライアント IP アドレスを知らなくてもクライアント接続を維持できるように、このオプションを無効にしてください。

次に、中央でスイッチングされる WLAN でクライアント IP アドレスの学習をディセーブルにする例を示します。

```
(Cisco Controller) >config wlan learn-ipaddr-cswlan 2 enable
```

関連コマンド

show wlan

config wlan load-balance

グローバル ロードバランシングの設定をオーバーライドし、特定の WLAN でロードバランシングをイネーブルまたはディセーブルにするには、**config wlan load-balance** コマンドを使用します。

config wlan load-balance allow {**enable** | **disable**} *wlan_id*

構文の説明

enable	無線 LAN で帯域選択をイネーブルにします。
disable	無線 LAN で帯域選択をディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

ロード バランシングはデフォルトではイネーブルになっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 3 の無線 LAN で帯域選択をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan load-balance allow enable 3
```

config wlan mac-filtering

無線 LAN で MAC フィルタリングの状態を変更するには、**config wlan mac-filtering** コマンドを使用します。

config wlan mac-filtering {**enable** | **disable**} {*wlan_id* | **foreignAp**}

構文の説明

enable	無線 LAN で MAC フィルタリングをイネーブルにします。
disable	無線 LAN で MAC フィルタリングをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 1 で MAC フィルタリングをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan mac-filtering enable 1
```

config wlan max-associated-clients

無線LAN、ゲストLAN、またはリモートLANのクライアント接続の最大数を設定するには、**config wlan max-associated-clients** コマンドを使用します。

config wlan max-associated-clients *max_clients wlan_id*

構文の説明

max_clients	許可されるクライアント接続の最大数。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 2 のクライアント接続の最大数を指定する例を示します。

```
(Cisco Controller) >config wlan max-associated-clients 25 2
```

config wlan max-radio-clients

アクセス ポイントごとの WLAN クライアントの最大数を設定するには、**config wlan max-radio-clients** コマンドを使用します。

config wlan max-radio-clients *max_radio_clients wlan_id*

構文の説明

max_radio_clients	無線アクセス ポイントあたりに許可されるクライアント接続の最大数。有効値は 1 ～ 200 です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 2 で、無線アクセス ポイントあたりのクライアント接続の最大数を指定する例を示します。

```
(Cisco Controller) >config wlan max-radio-clients 25 2
```

config wlan mdns

WLAN のマルチキャスト DNS（mDNS）プロファイルを設定するには、**config wlan mdns** コマンドを使用します。

config wlan mdns {**enable** | **disable** | **profile** {*profile-name* | **none**}} {*wlan_id* | **all**}

構文の説明

enable	WLAN で mDNS スヌーピングをイネーブルにします。
disable	WLAN で mDNS スヌーピングをディセーブルにします。
profile	WLAN の mDNS プロファイルを設定します。
profile-name	WLAN に関連付ける mDNS プロファイルの名前。
none	WLAN から既存の mDNS プロファイルを削除します。WLAN に mDNS プロファイルを設定できません。
wlan_id	1 ～ 512 の無線 LAN 識別子。
all	すべての WLAN の mDNS プロファイルを設定します。

コマンド デフォルト

デフォルトでは、WLAN で mDNS スヌーピングが有効になっています。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLANをディセーブルにします。クライアントはプロファイルに関連付けられたサービスのみのサービスアドバタイズメントを受信します。コントローラはインターフェイス グループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイス プロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。

次に、WLAN の mDNS プロファイルを設定する例を示します。

```
(Cisco Controller) >config wlan mdns profile profile1 1
```

config wlan media-stream

無線 LAN メディア ストリームのマルチキャスト ダイレクトを設定するには、**config wlan media-stream** コマンドを使用します。

config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

構文の説明

multicast-direct	無線 LAN メディア ストリームのマルチキャスト ダイレクトを設定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
all	すべてのメディア ストリームで無線 LAN を設定します。
enable	ユニキャスト変換するグローバル マルチキャストを有効にします。
disable	ユニキャスト変換するグローバル マルチキャストを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。WLAN Quality of Service（QoS）を gold または platinum のいずれかに設定する必要があります。

次に、WLAN ID 2 によってグローバル マルチキャスト ダイレクト メディア ストリームを有効にする例を示します。

```
(Cisco Controller) >config wlan media-stream multicast-direct 2 enable
```

config wlan mfp

無線 LAN に管理フレーム保護（MFP）オプションを設定するには、**config wlan mfp** コマンドを使用します。

config wlan mfp {**client** [**enable** | **disable**] *wlan_id* | **infrastructure protection** [**enable** | **disable**] *wlan_id*}

構文の説明

client	無線LANにクライアントMFPを設定します。
enable	（任意）機能をイネーブルにします。
disable	（任意）機能をディセーブルにします。
wlan_id	無線 LAN 識別子（1～512）。
infrastructure protection	（任意）無線 LAN にインフラストラクチャ MFP を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 1 のクライアント管理フレームの保護を設定する例を示します。

```
(Cisco Controller) >config wlan mfp client enable 1
```

config wlan mobility anchor

無線 LAN で MAC フィルタリングの状態を変更するには、**config wlan mobility anchor** コマンドを使用します。

config wlan mobility anchor {**add** | **delete**} *wlan_id ip_addr* **priority** *priority-number*

構文の説明

add	無線 LAN で MAC フィルタリングをイネーブルにします。
delete	無線 LAN で MAC フィルタリングをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
ip_addr	無線 LAN をアンカーするメンバ スイッチの IPv4 アドレス。
priority	アンカーされたワイヤレス LAN の IP アドレスに優先順位を設定します。
priority-number	範囲は 1 ~ 3 の間です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、 IPv4 アドレス形式のみをサポートします。
8.1	**priority***priority number* パラメータが導入されました。

次に、WLAN ID 4 と IPv4 アドレス 192.168.0.14 で、モビリティ無線 LAN アンカー リストに優先順位を設定する例を示します。

```
(Cisco Controller) >config wlan mobility anchor add 4 192.168.0.14 priority 1
```

関連コマンド

show wlan

config wlan mobility foreign-map

外部 Cisco WLC のインターフェイスまたはインターフェイス グループを設定するには、**config wlan mobility foreign-map** コマンドを使用します。

config wlan mobility foreign-map {**add** | **delete**} *wlan_id foreign_mac_address* {*interface_name* | *interface_group_name*}

構文の説明

add	外部コントローラ マップにインターフェイスまたはインターフェイス グループを追加します。
delete	外部コントローラ マップからインターフェイスまたはインターフェイス グループを削除します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreign_mac_address	WLAN の外部スイッチの MAC アドレス。
interface_name	最大 32 文字の英数字のインターフェイス名。
interface_group_name	最大 32 文字の英数字のインターフェイス グループ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 4 の Cisco WLC に対するインターフェイス グループと、WLAN 00:21:1b:ea:36:60 の外部スイッチの MAC アドレスを追加する例を示します。

```
(Cisco Controller) >config wlan mobility foreign-map add 4 00:21:1b:ea:36:60 mygroup1
```

config wlan multicast buffer

無線マルチキャスト パケット バッファ サイズを設定するには、**config wlan multicast buffer** コマンドを使用します。

config wlan multicast buffer {**enable** | **disable**} *buffer-size*

構文の説明

enable	無線 LAN のマルチキャスト インターフェイス機能をイネーブルにします。
disable	無線 LAN のマルチキャスト インターフェイス機能をディセーブルにします。
buffer-size	無線マルチキャスト パケット バッファ サイズ。範囲は 30 ～ 60 です。AP がマルチキャストに割り当てられるバッファ数を動的に調整することを指定するには、0 を入力します。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

デフォルトのバッファ サイズは 30 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、無線マルチキャスト バッファを設定する例を示します。

```
(Cisco Controller) >config wlan multicast buffer enable 45 222
```

config wlan multicast interface

無線 LAN にマルチキャスト インターフェイスを設定するには、**config wlan multicast interface** コマンドを使用します。

config wlan multicast interface *wlan_id* {**enable** | **disable**} *interface_name*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
enable	無線 LAN のマルチキャスト インターフェイス機能をイネーブルにします。
delete	無線 LAN のマルチキャスト インターフェイス機能をディセーブルにします。
interface_name	インターフェイス名。 （注） インターフェイス名は、小文字でしか指定できません。

コマンド デフォルト

マルチキャストはディセーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 4 およびインターフェイス名 myinterface1 の無線 LAN のマルチキャスト インターフェイス機能をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan multicast interface 4 enable myinterface1
```

config wlan mu-mimo

WLAN でマルチユーザ Multiple-Input Multiple-Output（MU-MIMO）を有効にするには、**config wlan mu-mimo** コマンドを入力します。

config wlan mu-mimo {**enable** | **disable**} *wlan-id*

構文の説明

enable *wlan-id*	指定された WLAN で MU-MIMO を有効にします
disable *wlan-id*	指定された WLAN で MU-MIMO を無効にします

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

config wlan nac

WLAN に対するネットワーク アドミッション コントロール（NAC）のアウトオブバンド サポートをイネーブルまたはディセーブルにするには、**config wlan nac** コマンドを使用します。

config wlan nac {**snmp** | **radius**} {**enable** | **disable**} *wlan_id*

構文の説明

snmp	SNMP NAC サポートを設定します。
radius	RADIUS NAC サポートを設定します。
enable	WLAN で NAC をイネーブルにします。
disable	WLAN で NAC をディセーブルにします。
wlan_id	1～512 の WLAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

RADIUS NAC 状態を有効にする前に、AAA オーバーライドを有効にする必要があります。RADIUS NAC 状態をイネーブルにする前に、FlexConnect ローカル スイッチングをディセーブルにする必要があります。

次に、WLAN 13 の SNMP NAC サポートを設定する例を示します。

```
(Cisco Controller) >config wlan nac snmp enable 13
```

次に、WLAN 34 の RADIUS NAC サポートを設定する例を示します。

```
(Cisco Controller) >config wlan nac radius enable 20
```

config wlan override-rate-limit

QoS プロファイルで定義されたユーザおよび Service Set Identifier（SSID）ごとに、アップストリームおよびダウンストリームの帯域幅制限をオーバーライドするには、 **config wlan override-rate-limit** コマンドを使用します。

config wlan override-rate-limit *wlan_id* { **average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate** } { **per-ssid** | **per-client** } { **downstream** | **upstream** } *rate*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
average-data-rate	ユーザまたは SSID ごとに TCP トラフィックの平均データ レートを指定します。範囲は 0 ～ 51,2000 Kbps です。
average-realtime-rate	ユーザまたは SSID ごとに UDP トラフィックの平均リアルタイム データ レートを指定します。範囲は 0 ～ 51,2000 Kbps です。
burst-data-rate	ユーザまたは SSID ごとに TCP トラフィックのピーク データ レートを指定します。範囲は 0 ～ 51,2000 Kbps です。
burst-realtime-rate	ユーザまたは SSID ごとに UDP トラフィックのピーク リアルタイムデータ レートを指定します。範囲は 0 ～ 51,2000 Kbps です。
per-ssid	無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。
per-client	SSID に関連付けられた各クライアントのレート制限を設定します。
downstream	ダウンストリーム トラフィックのレート制限を設定します。
upstream	アップストリーム トラフィックのレート制限を設定します。
rate	ユーザまたは SSID ごとの TCP または UDP トラフィックのデータ レート。範囲は 0 ～ 51,2000 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

レート制限は、コントローラと AP によって適用されます。中央スイッチングのために、コントローラは、ダウンストリームに対するクライアントごとのレート制限の適用を処理し、AP はアップストリーム トラフィックと、ダウンストリーム トラフィックに対する SSID ごとのレート制限の適用を処理します。AP は、スタンドアロン モードになったときに、ダウンストリームに対するクライアントごとのレート制限の適用も処理します。

FlexConnect ローカル スイッチング モードおよびスタンドアロン モードで、クライアントごと、SSID ごとのレート制限は、ダウンストリームおよびアップストリーム トラフィックに対して、AP によって実行されます。ただし、FlexConnect スタンドアロン モードの設定は AP に保存されないため、AP をリロードしたときに設定が失われ、レート制限は再起動後に適用されません。

ローミング クライアントが同じコントローラ上の AP 間でローミングする場合は、同じレート制限パラメータがクライアントに適用されます。ただし、クライアントがアンカー コントローラから外部コントローラへローミングする場合、クライアントごとのダウンストリーム レート制限では、アンカー コントローラで設定されたパラメータが使用され、アップストリーム レート制限では、外部コントローラーのパラメータが使用されます。

次に、SSID ごとにアップストリーム トラフィックに対して 2000 kbps Burst Real-time の実際のレートを設定する例を示します。

```
(Cisco Controller) >config wlan override-rate-limit 2 burst-realtime-rate per-ssid
upstream 2000
```

config wlan passive-client

無線 LAN のパッシブクライアント機能を設定するには、**config wlan passive-client** コマンドを使用します。

config wlan passive-client {**enable** | **disable**} *wlan_id*

構文の説明

enable	WLAN のパッシブクライアント機能をイネーブルにします。
disable	WLANのパッシブクライアント機能をディセーブルにします。
wlan_id	1 ～ 512 の WLAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを入力する前に、**config network multicast global** および **config network multicast mode** コマンドを使用して、グローバル マルチキャスト モードとマルチキャスト-マルチキャスト モードを有効にする必要があります。

（注） マルチキャストマルチキャスト モードのマルチキャストは、ユニキャスト モード以外のみで設定する必要があります。このリリースで、パッシブ クライアント機能は、マルチキャストユニキャスト モードで動作しません。

次に、無線 LAN ID 2 のパッシブ クライアントを設定する例を示します。

```
(Cisco Controller) >config wlan passive-client enable 2
```

config wlan peer-blocking

WLAN にピアツーピア ブロッキング機能を設定するには、**config wlan peer-blocking** コマンドを使用します。

config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

構文の説明

disable	ピアツーピア ブロッキングをディセーブルにして、可能な場合にはコントローラ内でトラフィックをローカルにブリッジします。
drop	コントローラでパケットを破棄するようにします。
forward-upstream	パケットがアップストリーム VLAN に転送されるようにします。これらのパケットに対して行われる動作は、コントローラよりも上流にあるデバイスにより決定されます。
wlan_id	1 ～ 512 の WLAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 1 のピアツーピア ブロッキングをディセーブルにする例を示します。

```
(Cisco Controller) >config wlan peer-blocking disable 1
```

config wlan pmipv6 default-realm

PMIPv6 WLAN のデフォルト レルムを設定するには、 **config wlan pmipv6 default-realm** コマンドを使用します。

config wlan pmipv6 default-realm { *default-realm-name* | **none** } *wlan_id*

構文の説明

default-realm-name	WLAN のデフォルトのレルム名。
none	WLAN のレルム名をクリアします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、PMIPv6 WLAN のデフォルト レルム名を設定する例を示します。

```
(Cisco Controller) >config wlan pmipv6 default-realm XYZ 6
```

config wlan pmipv6 mobility-type

WLAN のモビリティのタイプを設定するには、 **config wlan pmipv6 mobility-type** コマンドを使用します。

config wlan pmipv6 mobility-type {**none** | **pmipv6** } { *wlan_id* | **all** }

構文の説明

none	簡易 IP モビリティで WLAN を設定します。
pmipv6	PMIPv6 モビリティで WLAN を設定します。
all	すべての WLAN に対して、指定したモビリティのタイプをイネーブルにします。
wlan_id	1 ～ 512 の WLAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

モビリティのタイプを設定する場合は、WLAN をディセーブルにする必要があります。

次に、WLAN で PMIPv6 としてモビリティのタイプを設定する例を示します。

```
(Cisco Controller) >config wlan pmipv6 mobility-type pmipv6 16
```

config wlan pmipv6 profile_name

PMIPv6 WLAN のプロファイル名を設定するには、 **config wlan pmipv6 profile_name** コマンドを使用します。

config wlan pmipv6 profile_name *profile_name wlan_id*

構文の説明

profile_name	PMIPv6 WLAN のプロファイル名。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは PMIPv6 WLAN または SSID にプロファイル名をバインドします。モバイル ノードをコントローラに関連付けるたびに、PMIPV6 モジュールのトリガーにプロファイル名および NAI が使用されます。PMIPV6 モジュールは、LMA IP、APN、NAI など、すべてのプロファイル固有のパラメータを抽出し、PBU を ASR5K に送信します。

次に、PMIPv6 WLAN で ABC01 という名前のプロファイルを作成する例を示します。

```
(Cisco Controller) >config wlan pmipv6 profile_name ABC01 16
```

config wlan policy

WLAN でポリシーを設定するには、**config wlan policy** コマンドを使用します。

config wlan policy {**add** | **delete**} *priority-index wlan-id*

構文の説明

add	WLAN にポリシーを追加します。
delete	WLAN から既存のポリシーを削除します。
priority-index	WLAN で設定するポリシーの優先順位インデックス。ポリシーは、優先順位インデックスに従ってクライアントに適用されます。指定できる範囲は 1 ～ 16 です。
policy_name	プロファイルのポリシーの名前。
wlan-id	1～512 の WLAN 識別子。

コマンド デフォルト

WLAN ポリシーはありません。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

WLAN に対して最大 16 のポリシーを適用できます。

次に、WLAN にポリシーを設定する例を示します。

```
(Cisco Controller) >config wlan policy add 1 teacher_policy 1
```

config wlan profile

WLAN に関連付けられているプロファイルを編集するには、**config wlan profile** コマンドを使用します。

config wlan profile *wlan_id profile-name*

構文の説明

wlan_id	1～512 の WLAN 識別子。
profile-name	WLAN プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、WLAN に関連付けられているプロファイルを編集する例を示します。

```
(Cisco Controller) > config wlan disable 1
(Cisco Controller) > config wlan profile 1 new_sample
(Cisco Controller) > show wlan summary

Number of WLANs.................................. 1

WLAN ID  WLAN Profile Name / SSID    Status    Interface Name    PMIPv6 Mobility
-------  -------------------------   --------  ---------------   ---------------
1        new_sample / new_samp       Disabled  management            none
```

config wlan profiling

WLAN でクライアント プロファイリングを設定するには、**config wlan profiling** コマンドを使用します。

config wlan profiling {**local** | **radius**} {**all** | **dhcp** | **http**} {**enable** | **disable**} *wlan_id*

構文の説明

local	WLAN のローカル モードでクライアント プロファイリングを設定します。
radius	WLAN 上の RADIUS モードでクライアント プロファイリングを設定します。
all	WLAN で DHCP および HTTP クライアント プロファイリングを設定します。
dhcp	WLAN で、DHCP クライアント プロファイリングだけを設定します。
http	WLAN で、HTTP クライアント プロファイリングを設定します。
enable	WLAN で、クライアント プロファイリングの特定のタイプをイネーブルにします。 HTTP プロファイリングをイネーブルにすると、Cisco WLC は、プロファイリングのために、クライアントの HTTP 属性を収集します。 DHCP プロファイリングをイネーブルにすると、Cisco WLC は、プロファイリングのために、クライアントの DHCP 属性を収集します。
disable	WLAN で、クライアント プロファイリングの特定のタイプをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

使用上のガイドライン

WLAN のクライアント プロファイリングを設定する前に、WLAN をディセーブルにしたことを確認します。

コマンド デフォルト

クライアントのプロファイリングは無効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

HTTP でポート 80 に接続されたクライアントだけをプロファイリングできます。IPv6 専用クライアントはプロファイリングされません。

セッション タイムアウトが WLAN に対して設定されている場合、クライアントは、設定されたタイムアウトがプロファイリングされる前に HTTP トラフィックを送信する必要があります。

この機能は、以下ではサポートされていません。

- FlexConnect スタンドアロン モード
- FlexConnect ローカル認証

次に、WLAN で DHCP プロファイリングと HTTP プロファイリングの両方をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan profiling radius all enable 6
         HTTP Profiling successfully enabled.
         DHCP Profiling successfully enabled.
```

config wlan qos

無線 LAN の Quality Of Service（QoS）を変更するには、**config wlan qos** コマンドを使用します。

config wlan qos *wlan_id* {**bronze** | **silver** | **gold** | **platinum**}
config wlan qos foreignAp {**bronze** | **silver** | **gold** | **platinum**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
bronze	Bronze QoS ポリシーを指定します。
silver	Silver QoS ポリシーを指定します。
gold	Gold QoS ポリシーを指定します。
platinum	Platinum QoS ポリシーを指定します。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

デフォルトの QoS ポリシーはシルバーです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、無線 LAN 1 に最高レベルのサービスを設定する例を示します。

```
(Cisco Controller) >config wlan qos 1 gold
```

config wlan radio

無線LANにシスコの無線ポリシーを設定するには、**config wlan radio** コマンドを使用します。

config wlan radio *wlan_id* {**all** | **802.11a** | **802.11bg** | **802.11g** | **802.11ag**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
all	すべての無線帯域で無線LANを設定します。
802.11a	802.11a だけに無線 LAN を設定します。
802.11bg	802.11b/g だけに無線 LAN を設定します（802.11g がディセーブルな場合は 802.11b だけに設定）。
802.11g	802.11g だけに無線 LAN を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての無線帯域に無線 LAN を設定する例を示します。

```
(Cisco Controller) >config wlan radio 1 all
```

config wlan radius_server acct

WLAN で RADIUS アカウンティング サーバを設定するには、**config wlan radius_server acct** コマンドを使用します。

config wlan radius_server acct {**enable** | **disable**} *wlan_id* | **add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*} | **framed-ipv6** { **address** | **both** | **prefix** } *wlan_id*}

構文の説明

enable	WLAN の RADIUS アカウンティングをイネーブルにします。
disable	WLAN の RADIUS アカウンティングをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
add	設定されている RADIUS アカウンティング サーバへのリンクを追加します。
server_id	RADIUS サーバ インデックス。
delete	設定されている RADIUS アカウンティング サーバへのリンクを削除します。
address	IPv6 アドレスにアカウンティング フレーム化された IPv6 属性を設定します。
both	IPv6アドレスとプレフィックスにアカウンティング フレーム化された IPv6 属性を設定します。
prefix	IPv6 プレフィックスにアカウンティング フレーム化された IPv6 属性を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN 2 の RADIUS アカウンティングをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan radius_server acct enable 2
```

次に、設定された RADIUS アカウンティング サーバへのリンクを追加する例を示します。

```
(Cisco Controller) > config wlan radius_server acct add 2 5
```

config wlan radius_server acct interim-update

WLAN で RADIUS アカウンティング サーバの中間アップデートを設定するには、**config wlan radius_server acct interim-update** コマンドを使用します。

config wlan radius_server acct interim-update {**enable** | **disable** | *interval*} *wlan_id*

構文の説明

interim-update	RADIUS アカウンティング サーバの中間アップデートを設定します。
enable	WLAN の RADIUS アカウンティング サーバの中間アップデートをイネーブルにします。
disable	WLAN の RADIUS アカウンティング サーバの中間アップデートをディセーブルにします。
interval	ユーザが指定する中間アップデート間隔。有効な範囲は 180～3600 秒です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

RADIUS アカウンティング サーバの中間アップデートは 600 秒に設定されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN 2 の RADIUS アカウンティング サーバに 200 秒の中間アップデートを指定する例を示します。

```
(Cisco Controller) >config wlan radius_server acct interim-update 200 2
```

config wlan radius_server auth

WLAN で RADIUS 認証サーバを設定するには、**config wlan radius_server auth** コマンドを使用します。

config wlan radius_server auth {**enable** *wlan_id* | **disable** *wlan_id*} {**add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*}}

構文の説明

auth	RADIUS 認証を設定します
enable	この WLAN に対して RADIUS 認証をイネーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
disable	この WLAN に対して RADIUS 認証をディセーブルにします。
add	設定されている RADIUS サーバへのリンクを追加します。
server_id	RADIUS サーバ インデックス。
delete	設定されている RADIUS サーバへのリンクを削除します。
all	設定されている RADIUS サーバへのすべてのリンクを削除します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 1 およびサーバ ID 1 の設定済み RADIUS 認証サーバにリンクを追加する例を示します。

```
(Cisco Controller) >config wlan radius_server auth add 1 1
```

config wlan radius_server overwrite-interface

無線 LAN の RADIUS 動的インターフェイスを設定するには、**config wlan radius_server overwrite-interface** コマンドを使用します。

config wlan radius_server overwrite-interface {**enable** | **disable**} *wlan_id*

構文の説明

enable	この WLAN に対して RADIUS 動的インターフェイスをイネーブルにします。
disable	この WLAN に対して RADIUS 動的インターフェイスをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラは、ID として管理インターフェイスを使用します。RADIUS サーバが直接接続された動的インターフェイスにある場合、トラフィックは動的インターフェイスから送信されます。それ以外の場合は、管理 IP アドレスが使用されます。

この機能を有効にすると、コントローラは、その WLAN 上のすべての RADIUS 関連トラフィックの Identity および送信元として、WLAN の設定に指定されたインターフェイスを Identity として使用します。

次に、ID 1 の WLAN に対して RADIUS 動的インターフェイスをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan radius_server overwrite-interface enable 1
```

config wlan radius_server realm

WLAN でレルムを設定するには、**config wlan radius_server realm** コマンドを使用します。

config wlan *radius_server***realm** {**enable** | **disable**} *wlan-id*

構文の説明

radius_server	RADIUS サーバ インデックス。範囲は 1 ～ 17 です。
enable	WLAN でレルムを有効にします。
disable	WLAN でレルムを無効にします。
wlan-id	WLAN ID。範囲は 1 ～ 512 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、WLAN でレルムをイネーブルにする例を示します。

```
(Cisco Controller) > config wlan 2 realm enable 50
```

config wlan roamed-voice-client re-anchor

ローミングされる音声クライアントのリアンカー ポリシーを設定するには、**config wlan roamed-voice-client re-anchor** コマンドを使用します。

config wlan roamed-voice-client re-anchor {**enable** | **disable**} *wlan_id*

構文の説明

enable	ローミングされるクライアントのリアンカー ポリシーをイネーブルにします。
disable	ローミングされるクライアントのリアンカー ポリシーをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

ローミングされるクライアントのリアンカー ポリシーは無効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID が 1 のローミングされる音声クライアントで、リアンカー ポリシーをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan roamed-voice-client re-anchor enable 1
```

config wlan security 802.1X

無線 LAN のシスコ無線の 802.1X セキュリティの状態を変更するには、**config wlan security 802.1X** コマンドを使用します。

config wlan security 802.1X {**enable** {*wlan_id* | **foreignAp**} | **disable** {*wlan_id* | **foreignAp**} | **encryption** {*wlan_id* | **foreignAp**} {**0** | **40** | **104**} | **on-macfilter-failure** {**enable** | **disable**}}

構文の説明

enable	802.1X 設定を有効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
disable	802.1X 設定を無効にします。
encryption	静的 WEP キーとインデックスを指定します。
0	WEP キーのサイズを 0（暗号化なし）に指定します。デフォルト値は 104 です。 （注） 無線 LAN 内のすべてのキーは、同じサイズでなければなりません。
40	WEP キーのサイズを 40 ビットに指定します。デフォルト値は 104 です。 （注） 無線 LAN 内のすべてのキーは、同じサイズでなければなりません。
104	WEP キーのサイズを 104 ビットに指定します。デフォルト値は 104 です。 （注） 無線 LAN 内のすべてのキーは、同じサイズでなければなりません。
on-macfilter-failure	MAC フィルタの失敗に対する 802.1X を設定します。
enable	MAC フィルタの失敗に対する 802.1X 認証を有効にします。
disable	MAC フィルタの失敗に対する 802.1X 認証を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

無線 LAN のシスコ無線の 802.1X セキュリティの暗号化レベルを変更するには、次のキー サイズを使用します。

- 0：802.1X 暗号化なし。
- 40：40/64 ビット暗号化。
- 104：104/128 ビット暗号化（これは、デフォルトの暗号化設定です）。

次に、WLAN ID 16 で 802.1X セキュリティを設定する例を示します。

```
(Cisco Controller) >config wlan security 802.1X enable 16
```

config wlan security ckip

無線 LAN に Cisco Key Integrity Protocol（CKIP）セキュリティ オプションを設定するには、**config wlan security ckip** コマンドを使用します。

config wlan security ckip {**enable** | **disable**} *wlan_id* [**akm psk set-key** {**hex** | **ascii**} {**40** | **104**} **key** *key_index wlan_id* | **mmh-mic** {**enable** | **disable**} *wlan_id* | **kp** {**enable** | **disable**} *wlan_id*]

構文の説明

enable	CKIP セキュリティを有効にします。
disable	CKIP セキュリティを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
akm psk set-key	（任意）CKIP 無線 LAN の暗号キー管理を設定します。
hex	16 進数の暗号キーを指定します。
ascii	ASCII の暗号キーを指定します。
40	CKIP WLAN の静的暗号キーの長さを 40 ビットに設定します。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。
104	CKIP WLAN の静的暗号キーの長さを 104 ビットに設定します。104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。
key	CKIP WLAN のキーの設定を指定します。
key_index	設定済み PSK キー インデックス。
mmh-mic	（任意）CKIP 無線 LAN のマルチモジュラ ハッシュ メッセージ整合性チェック（MMH MIC）検証を設定します。
kp	（任意）CKIP 無線 LAN のキー置換を設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN 03 の PSK キー インデックス 2 に 104 ビット（16 進数文字 26 字）の CKIP WLAN 暗号キーを設定する例を示します。

```
(Cisco Controller) >config wlan security ckip akm psk set-key hex 104 key 2 03
```

config wlan security cond-web-redir

条件付き Web リダイレクトを有効または無効にするには、**config wlan security cond-web-redir** コマンドを使用します。

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

構文の説明

enable	条件付き Web リダイレクトを有効にします。
disable	条件付き Web リダイレクトを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 2 で条件付き Web リダイレクトを有効にする例を示します。

```
(Cisco Controller) >config wlan security cond-web-redir enable 2
```

config wlan security eap-params

WLAN でローカル EAP タイマーを設定するには、**config wlan security eap-params** コマンドを使用します。

config wlan security eap-params { {**enable** | **disbale**} | **eapol-key-timeout***timeout* | **eap-key-retries** *retries* | **identity-request-timeout** *timeout* | **identity-request-retries** *retries* | **request-timeout** *timeout* | **request-retries** *retries*}*wlan_id*

構文の説明

{**enable** | **disable** }	SSID 固有の EAP タイムアウトまたは再試行を有効または無効にするように指定します。デフォルトでは、無効に設定されています。
eapol-key-timeout *timeout*	コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーの送信を試みる時間（200 ～ 5000 ミリ秒）を指定します。有効な範囲は 200 ～ 5000 ミリ秒です。 デフォルト値は 1000 ミリ秒です。
eapol-key-retries *retries*	コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーの送信を試みる最大回数（0～4回）を指定します。 デフォルト値は 2 です。
identity-request- timeout *timeout*	コントローラがローカル EAP を使用して WLAN 内部のワイヤレス クライアントに EAP ID 要求の送信を試みる時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
identity-request-retries *retries*	コントローラがローカル EAP を使用して WLAN 内部のワイヤレス クライアントに EAP ID 要求の再送信を試みる最大回数（0～4回）を指定します。 デフォルト値は 2 です。
request-timeout	コントローラがローカル EAP を使用して WLAN 内部のワイヤレス クライアントに EAP パラメータ要求の送信を試みる時間（1～120 秒）を指定します。 デフォルト値は 30 秒です。

request-retries*retries*	コントローラがローカル EAP を使用して WLAN 内部のワイヤレス クライアントに EAP パラメータ要求の再送信を試みる最大回数（0 ～ 20 回）を指定します。 デフォルト値は 2 です。
wlan-id	WLAN ID 番号。

コマンド デフォルト

デフォルトの EAPOL キー タイムアウトは 1000 ミリ秒です。

EAPOL キーの再試行回数のデフォルトは 2 です。

デフォルトの ID 要求タイムアウト値は 30 秒です。

デフォルトの ID 要求試行回数は 2 です。

デフォルトの要求タイムアウト値は 30 秒です。

デフォルトの要求試行回数は 2 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。

次に、WLAN で SSID 固有の EAP パラメータを有効にする例を示します。

```
(Cisco Controller) > config wlan security eap-params enable 4
```

次に、WLAN で EAPOL キー タイムアウト パラメータを設定する例を示します。

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

次に、WLAN で EAPOL キーの再試行回数を設定する例を示します。

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

config wlan security eap-passthru

外部オーセンティケータに 802.1X フレーム パス スルーを設定するには、**config wlan security eap-passthru** コマンドを使用します。

config wlan security eap-passthru {**enable** | **disable**} *wlan_id*

構文の説明

enable	外部オーセンティケータへの 802.1X フレーム パス スルーを有効にします。
disable	外部オーセンティケータへの 802.1X フレーム パス スルーを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 2 の外部オーセンティケータへの 802.1X フレーム パス スルーを有効にする例を示します。

```
(Cisco Controller) >config wlan security eap-passthru enable 2
```

config wlan security ft

802.11r 高速移行ローミング パラメータを設定するには、**config wlan security ft** コマンドを使用します。

config wlan security ft {**enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

構文の説明

enable	802.11r 高速移行ローミング サポートを有効にします。
disable	802.11r 高速移行ローミング サポートを無効にします。
reassociation-timeout	再アソシエーション期限の間隔を設定します。
timeout-in-seconds	再アソシエーションのタイムアウト値（秒単位）。有効範囲は 1 ～ 100 秒です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

使用上のガイドライン

先に進む前に、WLAN を無効にしたことを確認します。

次に、WLAN 2 で 802.11r 高速移行ローミング サポートを有効にする例を示します。

```
(Cisco Controller) >config wlan security ft enable 2
```

次に、WLAN 2 の 802.11r 高速移行ローミング サポートに対する再アソシエーションのタイムアウト値を 20 秒に設定する例を示します。

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

config wlan security ft over-the-ds

分散システム上の 802.11r 高速移行パラメータを設定するには、**config wlan security ft over-the-ds** コマンドを使用します。

config wlan security ft over-the-ds {**enable** | **disable**} *wlan_id*

構文の説明

enable	分散システム上の 802.11r 高速移行ローミング サポートを有効にします。
disable	分散システム上の 802.11r 高速移行ローミング サポートを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

イネーブル

使用上のガイドライン

先に進む前に、WLAN を無効にしたことを確認します。

802.11r 高速移行が WLAN で有効であることを確認します。

次に、WLAN ID 2 の分散システム上の 802.11r 高速移行ローミング サポートを有効にする例を示します。

```
(Cisco Controller) >config wlan security ft over-the-ds enable 2
```

config wlan security IPsec disable

IPSec セキュリティを無効にするには、**config wlan security IPsec disable** コマンドを使用します。

config wlan security IPsec disable {*wlan_id* | **foreignAp**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 16 の IPSec を無効にする例を示します。

```
(Cisco Controller) >config wlan security IPsec disable 16
```

config wlan security IPsec enable

IPSec セキュリティを有効にするには、**config wlan security IPsec enable** コマンドを使用します。

config wlan security IPsec enable {*wlan_id* | **foreignAp**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 16 の IPSec を有効にする例を示します。

```
(Cisco Controller) >config wlan security IPsec enable 16
```

config wlan security IPsec authentication

無線 LAN で使用する IPSec セキュリティ認証プロトコルを変更するには、**config wlan security IPsec authentication** コマンドを使用します。

config wlan security IPsec authentication {**hmac-md5** | **hmac-sha-1**} {*wlan_id* | **foreignAp**}

構文の説明

hmac-md5	IPSec HMAC-MD5 認証プロトコルを指定します。
hmac-sha-1	IPsec HMAC-SHA-1 認証プロトコルを指定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 1 の IPsec HMAC-SHA-1 セキュリティ認証パラメータを設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec authentication hmac-sha-1 1
```

config wlan security IPsec encryption

無線 LAN で使用する IPSec セキュリティ暗号化プロトコルを変更するには、**config wlan security IPsec encryption** コマンドを使用します。

config wlan security IPsec encryption {**3des** | **aes** | **des**} {*wlan_id* | **foreignAp**}

構文の説明

3des	IPSec 3DES 暗号化をイネーブルにします。
aes	IPsec AES 128 ビット暗号化を有効にします。
des	IPSec DES 暗号化をイネーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IPSec AES 暗号化を設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec encryption aes 1
```

config wlan security IPsec config

無線 LAN で使用する適切なインターネット キー交換（IKE）CFG-Mode パラメータを設定するには、**config wlan security IPsec config** コマンドを使用します。

config wlan security IPsec config qotd *ip_address* {*wlan_id* | **foreignAp**}

構文の説明

qotd	cfg-mode の quote-of-the day サーバ IP を設定します。
ip_address	cfg-mode の quote-of-the-day サーバ IP。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

IKE はセッション キー（暗号化および認証）の配布方式として、および VPN エンドポイントにデータの保護方法を提供する手法として使用されます。IKE はセキュリティ アソシエーション（SA）のバンドルを各接続に割り当てて、接続を追跡します。

次に、WLAN 1 の CFG-mode の quote-of-the-day サーバ IP 44.55.66.77 を設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec config qotd 44.55.66.77 1
```

config wlan security IPsec ike authentication

無線 LAN で使用する IPSec インターネット キー交換（IKE）認証プロトコルを変更するには、**config wlan security IPsec ike authentication** コマンドを使用します。

config wlan security IPsec ike authentication {**certificates** {*wlan_id* | **foreignAp**} | **pre-share-key** {*wlan_id* | **foreignAp**} *key* | **xauth-psk** {*wlan_id* | **foreignAp**} *key*}

構文の説明

certificates	IKE 認証モードを有効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
pre-share-key	事前共有キーを持つ IKE Xauth を有効にします。
xauth-psk	IKE 事前共有キーを有効にします。
key	事前共有および xauth-psk に必要なキー。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IKE 認証モードを設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike authentication certificates 16
```

config wlan security IPsec ike dh-group

無線 LAN で使用する IPSec インターネット キー交換（IKE）Diffie-Hellman グループを変更するには、**config wlan security IPsec ike dh-group** コマンドを使用します。

config wlan security IPsec ike dh-group {*wlan_id* | **foreignAp**} {**group-1** | **group-2** | **group-5**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
group-1	DH グループ 1（768 ビット）を指定します。
group-2	DH グループ 2（1024 ビット）を指定します。
group-5	DH グループ 5（1536 ビット）を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、グループ 1 の Diffe Hellman グループ パラメータを設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike dh-group 1 group-1
```

config wlan security IPsec ike lifetime

無線 LAN で使用する IPSec インターネット キー交換（IKE）ライフタイムを変更するには、**config wlan security IPsec ike lifetime** コマンドを使用します。

config wlan security IPsec ike lifetime {*wlan_id* | **foreignAp**} *seconds*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
seconds	1800 ～ 345600 の IKE ライフタイム（秒）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、無線 LAN で使用する IPSec IKE ライフタイムを設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike lifetime 1 1900
```

config wlan security IPsec ike phase1

無線LANで使用するIPSecインターネットキー交換（IKE）フェーズ1を変更するには、**config wlan security IPsec ike phase1** コマンドを使用します。

config wlan security IPsec ike phase1 {**aggressive** | **main**} {*wlan_id* | **foreignAp**}

構文の説明

aggressive	IKE アグレッシブ モードを有効にします。
main	IKE メイン モードを有効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IPSec IKE フェーズ 1 を変更する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike phase1 aggressive 16
```

config wlan security IPsec ike contivity

無線 LAN で Nortel の Contivity VPN クライアント サポートを変更するには、**config wlan security IPsec ike contivity** コマンドを使用します。

config wlan security IPsec ike contivity {**enable** | **disable**} {*wlan_id* | **foreignAp**}

構文の説明

enable	この WLAN に対する Contivity のサポートを有効にします。
disable	この WLAN に対する Contivity のサポートを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Contivity VPN クライアント サポートを変更する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike contivity enable 14
```

config wlan security wpa akm ft

802.11r高速移行802.1Xを使用して認証キー管理を設定するには、**config wlan security wpa akm ft** コマンドを使用します。

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout** *seconds*]] {**enable** | **disable**} *wlan_id*

構文の説明

over-the-air	（任意）802.11r高速移行地上波ローミング サポートを設定します。
over-the-ds	（任意）802.11r高速移行ローミングDSサポートを設定します。
psk	（任意）802.11r高速移行PSKサポートを設定します。
reassociation-timeout	（任意）再アソシエーションの期限間隔を設定します。 有効な範囲は1 ～ 100秒です。デフォルト値は20秒です。
seconds	再アソシエーションの期限間隔（秒単位）。
enable	802.11r 高速移行 802.1X サポートを有効にします。
disable	802.11r 高速移行 802.1X サポートを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、802.11r 高速移行を使用して認証キー管理を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security ft

802.11r 高速移行ローミング パラメータを設定するには、**config wlan security ft** コマンドを使用します。

config wlan security ft {**enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

構文の説明

enable	802.11r 高速移行ローミング サポートを有効にします。
disable	802.11r 高速移行ローミング サポートを無効にします。
reassociation-timeout	再アソシエーション期限の間隔を設定します。
timeout-in-seconds	再アソシエーションのタイムアウト値（秒単位）。有効範囲は 1 ～ 100 秒です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

使用上のガイドライン

先に進む前に、WLAN を無効にしたことを確認します。

次に、WLAN 2 で 802.11r 高速移行ローミング サポートを有効にする例を示します。

```
(Cisco Controller) >config wlan security ft enable 2
```

次に、WLAN 2 の 802.11r 高速移行ローミング サポートに対する再アソシエーションのタイムアウト値を 20 秒に設定する例を示します。

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

config wlan security passthru

無線 LAN で使用する IPSec パススルーを変更するには、**config wlan security passthru** コマンドを使用します。

config wlan security passthru {**enable** | **disable**} {*wlan_id* | **foreignAp**} [*ip_address*]

構文の説明

enable	IPSec パススルーを有効にします。
disable	IPSec パススルーを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
ip_address	（任意）VPN トンネルを終端している IPSec ゲートウェイ（ルータ）の IP アドレスを入力します。

コマンド デフォルト

なし

次に、無線 LAN で使用する IPSec パススルーを変更する例を示します。

```
(Cisco Controller) >config wlan security passthru enable 3 192.12.1.1
```

config wlan security pmf

WLAN の 802.11w 管理フレーム保護（MFP）を設定するには、**config wlan security pmf** コマンドを使用します。

config wlan security pmf {**disable** | **optional** | **required** | **association-comeback** *association-comeback_timeout* | **saquery-retrytimeout** *saquery-retry_timeout*} *wlan_id*

構文の説明

disable	WLAN の 802.11w MFP 保護を無効にします。
optional	WLAN の 802.11w MFP 保護を有効にします。
required	クライアントが WLAN の 802.11w MFP 保護をネゴシエートすることを要求します。
association-comeback	802.11w アソシエーション復帰時間を設定します。
association-comeback_timeout	アソシエーション復帰間隔（秒単位）。アソシエーションがステータス コード 30 によって拒否された後に、アソシエートされているクライアントがアソシエーションを再試行するまでに待機する必要がある時間間隔。ステータス コード 30 のメッセージは、「Association request rejected temporarily; Try again later」です。 範囲は、1 ～ 20 秒です。
saquery-retrytimeout	802.11w セキュリティ アソシエーション（SA）クエリ リトライ タイムアウトを設定します。
saquery-retry_timeout	アソシエーションを再試行する前に、すでにアソシエートされているクライアントへのアソシエーション応答で特定される時間間隔。アソシエーションの復帰期間中、この時間間隔により、クライアントが実際のクライアントであり、不正なクライアントではないかどうかが確認されます。クライアントがこの時間内に応答しない場合は、クライアントアソシエーションがコントローラから削除されます。指定できる範囲は 100 ～ 500 ミリ秒です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

デフォルトの SA クエリ リトライ タイムアウトは 200 ミリ秒です。

デフォルトのアソシエーション復帰タイムアウトは 1 秒です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

802.11w では、ブロードキャストまたはマルチキャストの堅牢な管理フレームを保護するために使用される Integrity Group Temporal Key（IGTK）が導入されています。IGTK は、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用するオーセンティケータ ステーション（コントローラ）によって割り当てられる、ランダムな値です。802.11w IGTK キーは、4 ウェイ ハンドシェイクを使用して取得され、レイヤ 2 で WPA または WPA2 セキュリティによって設定されている WLAN でのみ使用されます。

次に、WLAN の 802.11w MFP 保護を有効にする例を示します。

```
(Cisco Controller) > config wlan security pmf optional 1
```

次に、WLAN の SA クエリ リトライ タイムアウトを設定する例を示します。

```
(Cisco Controller) > config wlan security pmf saquery-retrytimeout 300 1
```

config wlan security splash-page-web-redir

スプラッシュ ページ Web リダイレクトを有効または無効にするには、**config wlan security splash-page-web-redir** コマンドを入力します。

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

構文の説明

enable	スプラッシュ ページ Web リダイレクトを有効にします。
disable	スプラッシュ ページ Web リダイレクトを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

スプラッシュ ページ Web リダイレクトは無効です。

次に、スプラッシュ ページ Web リダイレクトを有効にする例を示します。

```
(Cisco Controller) >config wlan security splash-page-web-redir enable 2
```

config wlan security static-wep-key authentication

無線 LAN で静的 Wired Equivalent Privacy（WEP）キー 802.11 認証を設定するには、**config wlan security static-wep-key authentication** コマンドを使用します。

config wlan security static-wep-key authentication {**shared-key** | **open**} *wlan_id*

構文の説明

shared-key	共有キー認証を有効にします。
open	オープン システム認証を有効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WLAN ID 1 の静的 WEP 共有キー認証を有効にする例を示します。

```
(Cisco Controller) >config wlan security static-wep-key authentication shared-key 1
```

config wlan security static-wep-key disable

静的 Wired Equivalent Privacy（WEP）キーの使用を無効にするには、**config wlan security static-wep-key disable** コマンドを使用します。

config wlan security static-wep-key disable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WLAN ID 1 の静的 WEP キーを無効にする例を示します。

```
(Cisco Controller) >config wlan security static-wep-key disable 1
```

config wlan security static-wep-key enable

静的 Wired Equivalent Privacy（WEP）キーの使用を有効にするには、**config wlan security static-wep-key enable** コマンドを使用します。

config wlan security static-wep-key enable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WLAN ID 1 の静的 WEK キーを有効にする例を示します。

```
(Cisco Controller) >config wlan security static-wep-key enable 1
```

config wlan security static-wep-key encryption

静的 Wired Equivalent Privacy（WEP）キーとインデックスを設定するには、**config wlan security static-wep-key encryption** コマンドを使用します。

config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key-index*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
40	暗号化レベルを 40 に指定します。
104	暗号化レベルを 104 に指定します。
hex	キー入力に16進数文字を使用するように指定します。
ascii	キー入力に ASCII 文字を使用するように指定します。
key	ASCII の WEP キー。
key-index	キー インデックス（1 ～ 4）。

コマンド デフォルト

なし

使用上のガイドライン

各無線 LAN に 1 つの一意な WEP キー インデックスを適用できます。WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの無線 LAN しか設定できません。

このコマンドを使用する前に、802.1X を無効にしてください。

次に、16 進数文字 0201702001 およびキー インデックス 2 を使用して WLAN ID 1 の静的 WEP キーを設定する例を示します。

```
(Cisco Controller) >config wlan security static-wep-key encryption 1 40 hex 0201702001
2
```

config wlan security tkip

Temporal Key Integrity Protocol（TKIP）Message Integrity Check（MIC）カウンターメジャー ホールドダウン タイマーを設定するには、**config wlan security tkip** コマンドを使用します。

config wlan security tkip hold-down *time wlan_id*

構文の説明

hold-down	TKIP MIC カウンターメジャー ホールドダウン タイマーを設定します。
time	TKIP MIC カウンターメジャー ホールドダウンの秒単位の時間。有効な範囲は 0 ～ 60 秒です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

デフォルトの TKIP カウンターメジャーは 60 秒に設定されます。

使用上のガイドライン

TKIP カウンターメジャー モードは、アクセス ポイントが 60 秒の期間内に 2 つの MIC エラーを受信した場合に発生することがあります。この状況が発生した場合、アクセスポイントは、802.11 無線にアソシエートされているすべての TKIP クライアントの認証を解除し、カウンターメジャー ホールドオフ時間のクライアントを阻止します。

次に、TKIP MIC カウンターメジャー ホールドダウン タイマーを設定する例を示します。

```
(Cisco Controller) >config wlan security tkip
```

config wlan usertimeout

WLANでアイドル状態のクライアントセッションのタイムアウトを設定するには、**config wlan usertimeout** コマンドを使用します。

config wlan usertimeout *timeout wlan_id*

構文の説明

timeout	WLANに対するアイドル状態のクライアントセッションのタイムアウト。クライアントにより送信されるトラフィックがしきい値を下回る場合、クライアントはタイムアウト時に削除されます。範囲は 15 ～ 100000 秒です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

デフォルトのクライアント セッション アイドル タイムアウトは 300 秒です。

使用上のガイドライン

ここで設定したタイムアウト値は、コマンド **config network usertimeout** を使用して定義するグローバル タイムアウトをオーバーライドします。

次に、WLAN でアイドル状態のクライアント セッションを設定する例を示します。

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan security web-auth

無線 LAN で使用する Web 認証のステータスを変更するには、**config wlan security web-auth** コマンドを使用します。

config wlan security web-auth {{**acl** | **enable** | **disable**} {*wlan_id* | **foreignAp**} [*acl_name* | **none**]} | {**on-macfilter-failure** *wlan_id*} | {**server-precedence** *wlan_id* | **local** | **ldap** | **radius**} | {**flexacl** *wlan_id* [*ipv4_acl_name* | **none**]} | {**ipv6 acl** *wlan_id* [*ipv6_acl_name* | **none**]} | {**mac-auth-server** {*ip_address wlan_id*}} | {**timeout** {*value_in_seconds wlan_id*}} | {**web-portal-server** {*ip_address wlan_id*}}

構文の説明

acl	アクセス コントロール リストを設定します。
enable	Web 認証を有効にします。
disable	Web 認証を無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
acl_name	（任意）ACL 名（最大 32 文字の英数字）。
none	（任意）ACL 名を指定しません。
on-macfilter-failure	MAC フィルタの失敗における Web 認証を有効にします。
server-precendence	Web 認証ユーザに対する認証サーバの優先順位を設定します。
local	サーバ タイプを指定します。
ldap	サーバ タイプを指定します。
radius	サーバ タイプを指定します。
flexacl	FlexConnect のアクセス コントロール リストを設定します。
ipv4_acl_name	（任意）IPv4 ACL の名前。最大 32 文字の英数字を入力できます。
ipv6_acl_name	（任意）IPv6 ACL の名前。最大 32 文字の英数字を入力できます。
ipv6	IPv6 関連パラメータを設定します。

mac-auth-server	WLAN の MAC 認証サーバを設定します。
timeout	Web 認証タイムアウトを設定します。
value_in_seconds	タイムアウト値（秒）。有効な範囲は 300 ～ 14400 秒です。
web-portal-server	WLAN の CMCC Web ポータルのサーバを設定します。

コマンド デフォルト

なし

次に、WLAN ID 1 および ACL03 という名前の ACL のセキュリティ ポリシーを設定する例を示します。

```
(Cisco Controller) >config wlan security web-auth acl 1 ACL03
```

config wlan security web-passthrough acl

アクセス コントロール リスト（ACL）を無線 LAN 定義に追加するには、**config wlan security web-passthrough acl** コマンドを使用します。

config wlan security web-passthrough acl {*wlan_id* | **foreignAp**} {*acl_name* | **none**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
acl_name	ACL 名（最大 32 文字の英数字）。
none	ACL がないことを指定します。

コマンド デフォルト

なし

次に、ACL を無線 LAN 定義に追加する例を示します。

```
(Cisco Controller) >config wlan security web-passthrough acl 1 ACL03
```

config wlan security web-passthrough disable

無線 LAN で認証不要の Web キャプティブ ポータルを無効にするには、**config wlan security web-passthrough disable** コマンドを使用します。

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

次に、無線 LAN ID 1 で認証不要の Web キャプティブ ポータルを無効にする例を示します。

```
(Cisco Controller) >config wlan security web-passthrough disable 1
```

config wlan security web-passthrough email-input

電子メールアドレスを使用してWebキャプティブ ポータルを設定するには、**config wlan security web-passthrough email-input** コマンドを使用します。

config wlan security web-passthrough email-input {**enable** | **disable**} {*wlan_id* | **foreignAp**}

構文の説明

email-input	電子メール アドレスを使用して Web キャプティブ ポータルを設定します。
enable	電子メール アドレスを使用して Web キャプティブ ポータルを有効にします。
disable	電子メール アドレスを使用して Web キャプティブ ポータルを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

次に、電子メール アドレスを使用して Web キャプティブ ポータルを設定する例を示します。

```
(Cisco Controller) >config wlan security web-passthrough email-input enable 1
```

config wlan security web-passthrough enable

無線 LAN で認証不要の Web キャプティブ ポータルを有効にするには、**config wlan security web-passthrough enable** コマンドを使用します。

config wlan security web-passthrough enable {*wlan_id* | **foreignAp**}

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。

コマンド デフォルト

なし

次に、無線 LAN ID 1 で認証不要の Web キャプティブ ポータルを有効にする例を示します。

```
(Cisco Controller) >config wlan security web-passthrough enable 1
```

config wlan security wpa akm 802.1x

802.1X を使用して認証キー管理（AKM）を設定するには、**config wlan security wpa akm 802.1x** コマンドを使用します。

config wlan security wpa akm 802.1x {**enable** | **disable**} *wlan_id*

構文の説明

enable	802.1X サポートを有効にします。
disable	802.1X サポートを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、802.1X を使用して認証を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm 802.1x enable 1
```

config wlan security wpa akm cckm

Cisco Centralized Key Management（CCKM）を使用して認証キー管理を設定するには、**config wlan security wpa akm cckm** コマンドを使用します。

config wlan security wpa akm cckm {**enable** *wlan_id* | **disable** *wlan_id* | *timestamp-tolerance* }

構文の説明

enable	CCKM サポートを有効にします。
disable	CCKM サポートを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。
timestamp-tolerance	CCKM IE のタイムスタンプのトレランス。有効な範囲は 1000 ～ 5000 ミリ秒です。デフォルトは 1000 ミリ秒です。

コマンド デフォルト

なし

次に、CCKM を使用して認証キー管理を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm cckm 1500
```

config wlan security wpa akm ft

802.11r高速移行802.1Xを使用して認証キー管理を設定するには、**config wlan security wpa akm ft** コマンドを使用します。

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout** *seconds*]] {**enable** | **disable**} *wlan_id*

構文の説明

over-the-air	（任意）802.11r高速移行地上波ローミング サポートを設定します。
over-the-ds	（任意）802.11r高速移行ローミングDSサポートを設定します。
psk	（任意）802.11r高速移行PSKサポートを設定します。
reassociation-timeout	（任意）再アソシエーションの期限間隔を設定します。 有効な範囲は1 ～ 100秒です。デフォルト値は20秒です。
seconds	再アソシエーションの期限間隔（秒単位）。
enable	802.11r 高速移行 802.1X サポートを有効にします。
disable	802.11r 高速移行 802.1X サポートを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、802.11r 高速移行を使用して認証キー管理を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security wpa akm pmf

管理フレームの認証キー管理（AKM）を設定するには、**config wlan security wpa akm pmf** コマンドを使用します。

config wlan security wpa akm pmf {**802.1x** | **psk**} {**enable** | **disable**}*wlan_id*

構文の説明

802.1x	管理フレームの保護（PMF）の802.1X認証を設定します。
psk	PMF の事前共有キー（PSK）を設定します。
enable	PMF の 802.1X 認証または PSK を有効にします。
disable	PMF の 802.1X 認証または PSK を無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

ディセーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

802.11w には、00-0F-AC:5 または 00-0F-AC:6 の 2 つの新しい AKM スイートがあります。WPA を有効にし、次に WLAN を無効にして WLAN 上で PMF を設定する必要があります。

次に、WLAN の PMF の 802.1X 認証を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa akm pmf 802.1x enable 1
```

config wlan security wpa akm psk

Wi-Fi Protected Access（WPA）事前共有キー モードを設定するには、**config wlan security wpa akm psk** コマンドを使用します。

config wlan security wpa akm psk {**enable** | **disable** | **set-key** *key-format key*} *wlan_id*

構文の説明

enable	WPA-PSK を有効にします。
disable	WPA-PSK を無効にします。
set-key	事前共有キーを設定します。
key-format	キー形式を指定します。ASCII または 16 進数のいずれかになります。
key	WPA 事前共有キー。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WPA 事前共有キー モードを設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm psk disable 1
```

config wlan security wpa disable

WPA1 を無効にするには、**config wlan security wpa disable** コマンドを使用します。

config wlan security wpa disable *wlan_id*

構文の説明		
	wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト なし

次に、WPA を無効にする例を示します。

```
(Cisco Controller) >config wlan security wpa disable 1
```

config wlan security wpa enable

WPA1 を有効にするには、**config wlan security wpa enable** コマンドを使用します。

config wlan security wpa enable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WLAN ID 1 で WPA を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa enable 1
```

config wlan security wpa ciphers

Wi-Fi 保護認証（WPA1）または Wi-Fi 保護認証（WPA2）を設定するには、**config wlan security wpa ciphers** コマンドを使用します。

config wlan security wpa {**wpa1** | **wpa2**} **ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

構文の説明

wpa1	WPA1 サポートを設定します。
wpa2	WPA2 サポートを設定します。
ciphers	WPA 暗号方式を設定します。
aes	AES 暗号化のサポートを設定します。
tkip	TKIP 暗号化のサポートを設定します。
enable	WPA AES/TKIP モードを有効にします。
disable	WPA AES/TKIP モードを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

使用上のガイドライン

WPA バージョンを指定しない場合は、次のようになります。

- 有効化された暗号が AES の場合、WPA2/AES を設定しています。
- 有効化された暗号が AES+TKIP の場合、WPA/TKIP、WPA2/AES、または WPA/TKIP を設定しています。
- 有効化された暗号が TKIP の場合、WPA/TKIP または WPA2/TKIP を設定しています。

、スタンドアロン暗号化方式として TKIP を設定できなくなりました。TKIP は、AES 暗号化方式でのみ使用できます。

次に、WPA を暗号化する例を示します。

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers aes enable 1
```

config wlan security wpa gtk-random

WLAN のアクセス ポイントとクライアントとの間で Group Temporal Key（GTK）のランダム化を有効にするには、**config wlan security wpa gtk-random** コマンドを使用します。

config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

構文の説明

enable	アクセスポイントとクライアント間の GTK キーのランダム化を有効にします。
disable	アクセスポイントとクライアント間の GTK キーのランダム化を無効にします。
wlan_id	1 ～ 512 の WLAN 識別子。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドを有効にすると、基本サービスセット（BSS）のクライアントに一意の GTK キーが提供されます。クライアントは、マルチキャスト トラフィックまたはブロードキャスト トラフィックを受信しません。

次に、WLAN でアソシエートされている各クライアントの GTK のランダム化を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa gtk-random enable 3
```

config wlan security wpa osen disable

WLAN で OSU Server-Only Authenticated L2 Encryption Network（OSEN）を無効にするには、WLAN コンフィギュレーション モードで **config wlan security wpa osen enable** コマンドを使用します。

config wlan security wpa osen disable *wlan-id*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。

コマンド デフォルト

OSEN が有効になります。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、WLAN で OSEN を無効にする例を示します。

```
Cisco Controller > config wlan security wpa osen disable 12
```

config wlan security wpa osen enable

WLAN で OSU Server-Only Authenticated L2 Encryption Network（OSEN）を有効にするには、WLAN コンフィギュレーション モードで **config wlan security wpa osen enable** コマンドを使用します。

config wlan security wpa osen enable *wlan-id*

構文の説明

wlan-id	WLAN ID 番号。1 ～ 512 の値を入力します。

コマンド デフォルト

OSEN が有効ではありません

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、WLAN で OSEN を有効にする例を示します。

```
Cisco Controller > config wlan security wpa osen enable 12
```

config wlan security wpa wpa1 disable

WPA1 を無効にするには、**config wlan security wpa wpa1 disable** コマンドを使用します。

config wlan security wpa wpa1 disable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WPA1 を無効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa1 disable 1
```

config wlan security wpa wpa1 enable

WPA1 を有効にするには、**config wlan security wpa wpa1 enable** コマンドを使用します。

config wlan security wpa wpa1 enable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WPA1 を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa1 enable 1
```

config wlan security wpa wpa2 disable

WPA2 を無効にするには、**config wlan security wpa wpa2 disable** コマンドを使用します。

config wlan security wpa wpa2 disable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WPA2 を無効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 disable 1
```

config wlan security wpa wpa2 enable

WPA2 を有効にするには、**config wlan security wpa wpa2 enable** コマンドを使用します。

config wlan security wpa wpa2 enable *wlan_id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WPA2 を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 enable 1
```

config wlan security wpa wpa2 cache

WLAN のキャッシュ方法を設定するには、 **config wlan security wpa wpa2 cache** コマンドを使用します。

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

構文の説明

sticky	WLAN の Sticky Key Caching（SKC）ローミング サポートを設定します。
enable	WLAN で SKC ローミング サポートを有効にします。
disable	WLAN で SKC ローミング サポートを無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

使用上のガイドライン

PKC（Pro Active Key caching）とも呼ばれる SKC（Sticky Key caching）では、クライアントは Pairwise Master Key Security Association（PMKSA）に対して各 Pairwise Master Key（PMK）ID（PMKID）を保存します。クライアントがそれに対する PMKSA を保持する AP を見つけた場合、アソシエーション要求内で PMKID を AP に送信します。PMKSA が AP で稼働している場合は、AP は、高速ローミングをサポートします。SKC では、クライアントがアソシエートする新しい AP に関して完全な認証が実行され、すべての AP とアソシエートされる PMKSA をクライアントが維持しなければなりません。

次に、WLAN の SKC ローミング サポートを有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 1
```

config wlan security wpa wpa2 cache sticky

WLAN の Sticky PMKID Caching（SKC）を設定するには、**config wlan security wpa wpa2 cache sticky** コマンドを使用します。

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

構文の説明

enable	WLAN で SKC を有効にします。
disable	WLAN で SKC を無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

Stkcky PMKID Caching は無効です。

使用上のガイドライン

Sticky PMKID Caching（SKC）をサポートします。sticky PMKID キャッシュにより、クライアントは、アソシエートする AP ごとに異なる PMKID を受信し、保存します。AP も、クライアントに発行される PMKID のデータベースを維持します。PKC（Proactive Key Caching）とも呼ばれる SKC では、クライアントは Pairwise Master Key Security Association（PMKSA）に対して各 Pairwise Master Key（PMK）ID（PMKID）を保存します。クライアントがそれに対する PMKSA を保持する AP を見つけた場合、アソシエーション要求内で PMKID を AP に送信します。PMKSA が AP で稼働している場合は、AP は、高速ローミングをサポートします。SKC では、クライアントがアソシエートする新しい AP に関して完全な認証が実行され、すべての AP とアソシエートされる PMKSA をクライアントが維持しなければなりません。SKC の場合、PMKSA はクライアントが保存する AP のキャッシュごとであり、新しい AP の BSSID に基づいて事前に計算されます。

- コントローラは最大 8 つの SKC しかサポートしていないため、大規模な展開に SKC を使用することはできません。
- SKC は、モビリティ グループのアクセス コントローラでは機能しません。
- SKC は、WPA2 が有効になっている WLAN でのみ動作します。
- SKC はローカル モードの AP でのみ動作します。

次に、WLAN 5 で Sticky PMKID Caching を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 5
```

config wlan security wpa wpa2 ciphers

WPA2 暗号方式を設定し、WPA2 の Advanced Encryption Standard（AES）または Temporal Key Integrity Protocol（TKIP）データ暗号化を有効または無効にするには、**config wlan security wpa wpa2 ciphers** コマンドを使用します。

config wlan security wpa wpa2 ciphers {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

構文の説明

(Cisco Controller) > **aes**	WPA2 に対する AES データ暗号化を設定します。
tkip	WPA2 に対する TKIP データ暗号化を設定します。
enable	WPA2 に対する AES または TKIP データ暗号化を有効にします。
disable	WPA2 の AES または TKIP データ暗号化を無効にします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

AES はデフォルトで有効です。

次に、WPA2 に対する AES データ暗号化を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

config wlan session-timeout

無線 LAN クライアントのタイムアウトを変更するには、**config wlan session-timeout** コマンドを使用します。

config wlan session-timeout {*wlan_id* | **foreignAp**} *seconds*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
foreignAp	サードパーティのアクセス ポイントを指定します。
seconds	タイムアウトまたはセッション時間（秒）。値 0 は、タイムアウトなしに相当します。 （注） セッション タイムアウトの範囲は、セキュリティ タイプによって異なります。 • オープン システム：0 ～ 65535（秒） • 802.1x：300 ～ 86400（秒） • Static WEP：0 ～ 65535（秒） • Cranite：0 ～ 65535（秒） • Fortress：0 ～ 65535（秒） • CKIP：0 ～ 65535（秒） • Open + Web Auth：0 ～ 65535（秒） • Web Pass-thru：0 ～ 65535（秒） • WPA-PSK：0 ～ 65535（秒） • disable：再認証/セッション タイムアウト タイマーを無効にします。

コマンド デフォルト

なし

使用上のガイドライン

PMK キャッシュを作成する 802.1x クライアント セキュリティ タイプでは、セッション タイムアウトが無効になっている場合、設定できる最大セッション タイムアウトは 86400 秒です。PMK キャッシュが作成されない、オープン、WebAuth、PSK などのその他のクライアント セキュリティでは、セッション タイムアウトが無効になっている場合、セッション タイムアウト値は [infinite] と表示されます。

次に、WLAN ID 1 に対してクライアントのタイムアウトを 6000 秒に設定する例を示します。

```
(Cisco Controller) >config wlan session-timeout 1 6000
```

config wlan sip-cac disassoc-client

セッション開始プロトコル（SIP）のコール アドミッション制御（CAC）の障害時にクライアントのディスアソシエーションをイネーブルにするには、**config wlan sip-cac disassoc-client** コマンドを使用します。

config wlan sip-cac disassoc-client {**enable** | **disable**} *wlan_id*

構文の説明

enable	SIP CAC 障害時のクライアントのディスアソシエーションをイネーブルにします。
disable	SIP CAC 障害時のクライアントのディスアソシエーションをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

SIP CAC のクライアントのディスアソシエーションがディセーブルです。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID が 1 である SIP CAC 障害時のクライアントのディスアソシエーションをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan sip-cac disassoc-client enable 1
```

config wlan sip-cac send-486busy

SIP コール アドミッション制御（CAC）の障害が発生した場合にセッション開始プロトコル（SIP）の 486 Busy メッセージを送信するように設定するには、**config wlan sip-cac send-486busy** コマンドを使用します。

config wlan sip-cac send-486busy {**enable** | **disable**} *wlan_id*

構文の説明

enable	SIP CAC 障害時の SIP 486 Busy メッセージの送信をイネーブルにします。
disable	SIP CAC 障害時の SIP 486 Busy メッセージの送信をディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

セッション開始プロトコルはデフォルトで有効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID が 1 である SIP CAC 障害時の SIP 486 Busy メッセージの送信をイネーブルにする方法を示します。

```
(Cisco Controller) >config wlan sip-cac send-busy486 enable 1
```

config wlan ssid

WLAN に関連付けられている SSID を編集するには、**config wlan ssid** コマンドを使用します。

config wlan ssid *wlan_id ssid*

構文の説明

wlan_id	1～512 の WLAN 識別子。
ssid	WLANに関連付けられているサービス セット識別子（SSID）。

コマンド デフォルト

なし

次に、WLAN に関連付けられている SSID を編集する例を示します。

```
(Cisco Controller) >config wlan disable 1
(Cisco Controller) >config wlan ssid 1 new_samp
(Cisco Controller) >show wlan summary
Number of WLANs.................................. 1

WLAN ID  WLAN Profile Name / SSID   Status    Interface Name   PMIPv6 Mobility
-------  -------------------------  -------  -----------------  ---------------
1        sample / new_samp          Disabled   management            none
```

config wlan static-ip tunneling

WLAN でスタティック IP クライアント トンネリングのサポートを設定するには、**config wlan static-ip tunneling** コマンドを使用します。

config wlan static-ip tunneling {**enable** | **disable**} *wlan_id*

構文の説明

tunneling	WLAN でスタティック IP クライアント トンネリングのサポートを設定します。
enable	WLAN でスタティック IP クライアント トンネリングのサポートをイネーブルにします。
disable	WLAN でスタティック IP クライアント トンネリングのサポートをディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WLAN ID 3 のスタティック IP クライアント トンネリングのサポートをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan static-ip tunneling enable 34
```

config wlan uapsd compliant client enable

WPA1 を有効にするには、**config wlan uapsd compliant-client enable** コマンドを使用します。

（注） これは Ascom WMM 非対応電話機向けに導入されたもので、Cisco 792x/9971 IP フォンには適用されません。

config wlan uapsd compliant-client enable*wlan-id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WPA1 を有効にする例を示します。

```
(Cisco Controller) >config wlan uapsd compliant-client enable 1
```

プロパティ タイプ	プロパティ値	プロパティの説明

config wlan uapsd compliant-client disable

WPA1 を無効にするには、**config wlan uapsd compliant-client disable** コマンドを使用します。

（注） これは Ascom WMM 非対応電話機向けに導入されたもので、Cisco 792x/9971 IP フォンには適用されません。

config wlan uapsd compliant-client disable*wlan-id*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

次に、WPA1 を有効にする例を示します。

```
(Cisco Controller) >config wlan uapsd compliant-client disable 1
```

config wlan user-idle-threshold

WLAN クライアント セッションのアイドル タイムアウト中に、クライアントから送信されるしきい値のデータを設定するには、**config wlan user-idle-threshold** コマンドを使用します。

config wlan user-idle-threshold *bytes wlan_id*

構文の説明

bytes	WLAN クライアント セッションのアイドル タイムアウト中にクライアントから送信されるしきい値のデータ。クライアントにより送信されるトラフィックが、定義されているしきい値を下回る場合、クライアントはタイムアウト時に削除されます。範囲は 0 ～ 10000000 バイトです。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

アイドルタイムアウト中に、クライアントによりしきい値データが送信されるデフォルトのタイムアウトは 0 バイトです。

次に、WLAN クライアント セッションのアイドル タイムアウト中にクライアントから送信されるしきい値データを設定する例を示します。

```
(Cisco Controller) >config wlan user-idle-threshold 100 1
```

config wlan usertimeout

WLANでアイドル状態のクライアントセッションのタイムアウトを設定するには、**config wlan usertimeout** コマンドを使用します。

config wlan usertimeout *timeout wlan_id*

構文の説明

timeout	WLANに対するアイドル状態のクライアントセッションのタイムアウト。クライアントにより送信されるトラフィックがしきい値を下回る場合、クライアントはタイムアウト時に削除されます。範囲は 15 ～ 100000 秒です。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

デフォルトのクライアント セッション アイドル タイムアウトは 300 秒です。

使用上のガイドライン

ここで設定したタイムアウト値は、コマンド **config network usertimeout** を使用して定義するグローバル タイムアウトをオーバーライドします。

次に、WLAN でアイドル状態のクライアント セッションを設定する例を示します。

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan webauth-exclude

Web 認証ポリシーが期限切れになった時点でゲスト ユーザの IP アドレスを解放し、3 分間 IP アドレスを取得できないよう、そのゲストユーザを除外するには、**config wlan webauth-exclude** コマンドを使用します。

config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

構文の説明

wlan_id	無線 LAN 識別子（1～512）。
enable	Web 認証の除外をイネーブルにします。
disable	Web 認証の除外をディセーブルにします。

コマンド デフォルト

ディセーブル

使用上のガイドライン

このコマンドは、Web 認証が設定されているゲスト WLAN に使用できます。

コントローラに内部 DHCP スコープを設定するときに、このコマンドを適用できます。

デフォルトでは、ゲスト ユーザの Web 認証タイマーが期限切れになった時点で、ゲスト ユーザは、別のゲスト ユーザがその IP アドレスを取得する前にただちに同じ IP アドレスを再アソシエートすることができます。DHCP プールに多数のゲスト ユーザまたは制限付きの IP アドレスが存在する場合、一部のゲスト ユーザが IP アドレスを取得できない場合があります。

ゲスト WLAN でこの機能を有効にすると、Web 認証ポリシーが期限切れになった時点でゲスト ユーザの IP アドレスが解放され、そのゲスト ユーザは IP アドレスを取得できないよう、3 分間除外されます。その IP アドレスは、別のゲスト ユーザが使用できます。3 分経過すると、除外されていたゲスト ユーザは再アソシエートし、可能であれば IP アドレスを取得できるようになります。

次に、WLAN ID 5 の Web 認証除外をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan webauth-exclude 5 enable
```

config wlan wifidirect

WLAN で Wi-Fi Direct クライアント ポリシーを設定するには、**config wlan wifidirect** コマンドを使用します。

config wlan wifidirect {**allow** | **disable** | **not-allow** | **xconnect-not-allow**} *wlan_id*

構文の説明

allow	Wi-Fi Direct クライアントと WLAN のアソシエーションを許可します。
disable	クライアントの Wi-Fi Direct ステータスを無視し、それによって Wi-Fi Direct クライアントのアソシエーションを許可します。
not-allow	Wi-Fi Direct クライアントと WLAN のアソシエーションを禁止します。
xconnect-not-allow	AP による、Wi-Fi Direct オプションが有効になっているクライアントのアソシエーションの許可を有効にしますが、クライアント（Wi-Fi 標準に従って動作する場合）は、ピアツーピア接続を差し控えます。
wlan_id	無線 LAN 識別子（1 ～ 16）。

コマンド デフォルト

なし

次に、WLAN ID 1 で Wi-Fi Direct クライアント ポリシーを許可する例を示します。

```
(Cisco Controller) >config wlan wifidirect allow 1
```

config wlan wmm

無線 LAN に Wi-Fi マルチメディア（WMM）モードを設定するには、**config wlan wmm** コマンドを使用します。

config wlan wmm {**allow** | **disable** | **require**} *wlan_id*

構文の説明

allow	無線 LAN で WMM を許可します。
disable	無線LANでWMMをディセーブルにします。
require	指定した無線LANでクライアントにWMMの使用を指定します。
wlan_id	無線 LAN 識別子（1～512）。

コマンド デフォルト

なし

使用上のガイドライン

コントローラがレイヤ2モードで、WMMが有効化されている場合にアクセス ポイントをコントローラに結合できるようにするには、これらのアクセス ポイントをトランク ポート上に配置する必要があります。

次に、WMM を許可にするように無線 LAN ID 1 を設定する例を示します。

```
(Cisco Controller) >config wlan wmm allow 1
```

次に、クライアントによる WMM の使用を指定するように無線 LAN ID 1 を設定する例を示します。

```
(Cisco Controller) >config wlan wmm require 1
```

config wps ap-authentication

アクセス ポイントのネイバー認証を設定するには、**config wps ap-authentication** コマンドを使用します。

config wps ap-authentication ［**enable** | **disable threshold** *threshold_value*］

構文の説明

enable	（任意）無線LANでWMMを有効にします。
disable	（任意）無線LANでWMMを無効にします。
threshold	（任意）無線LANのWMM対応クライアントであることを指定します。
threshold_value	しきい値（1 ～ 255）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、アクセス ポイント ネイバー認証を設定する例を示します。

```
(Cisco Controller) > config wps ap-authentication threshold 25
```

関連コマンド

show wps ap-authentication summary

config wps auto-immune

サービス拒否（DoS）攻撃からの保護を有効または無効にするには、**config wps auto-immune** コマンドを使用します。

config wps auto-immune {**enable** | **disable** | **stop**}

構文の説明

enable	自己免疫機能を有効にします。
disable	自己免疫機能を無効にします。
stop	ダイナミック自己免疫機能を停止します。

コマンド デフォルト

無効

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

潜在的な攻撃者は特別に作成したパケットを使用し、正規のクライアントを攻撃者として処理するように侵入検知システム（IDS）を誘導する場合があります。それによって、コントローラはこの正規のクライアントの接続を解除し、DoS 攻撃が開始されます。自己免疫機能は、有効な場合にこのような攻撃を防ぐように設計されています。ただし、自己免疫機能を有効にすると、Cisco 792x フォンを使用した会話が断続的に中断されることがあります。792x フォンを使用しているときに頻繁に中断されるようであれば、この機能を無効にしてください。

次に、自己免疫モードを設定する例を示します。

```
(Cisco Controller) > config wps auto-immune enable
```

次に、自己免疫モードを停止する例を示します。

```
(Cisco Controller) > config wps auto-immune stop
Dynamic Auto Immune by WIPS is stopped
```

関連コマンド

show wps summary

config wps cids-sensor

Wireless Protection System（WPS）の侵入検知システム（IDS）センサーを設定するには、**config wps cids-sensor** コマンドを使用します。

config wps cids-sensor ｛［**add** *index ip_address username password*］｜［**delete** *index*］｜［**enable** *index*］｜［**disable** *index*］｜［**port** *index port*］｜［**interval** *index query_interval*］｜［**fingerprint sha1** *fingerprint*］｝

構文の説明

add	（任意）新しい IDS センサーを設定します。
index	IDS センサーの内部インデックス。
ip_address	IDS センサーの IP アドレス。
username	IDS センサーのユーザ名。
password	IDS センサーのパスワード。
delete	（任意）IDS センサーを削除します。
enable	（任意）IDS センサーを有効にします。
disable	（任意）IDS センサーを無効にします。
port	（任意）IDS センサーのポート番号を設定します。
port	ポート番号。
interval	（任意）IDS センサーのクエリ間隔を指定します。
query_interval	クエリ間隔の設定。
fingerprint	（任意）IDS センサーの TLS フィンガープリントを指定します。
sha1	（任意）TLS フィンガープリントを指定します。
fingerprint	TLS フィンガープリント。

コマンド デフォルト

コマンドのデフォルトを次に示します。

ポート	443
クエリー インターバル	60

認証フィンガープリント	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
クエリー状態	無効

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IDS インデックス 1、IDS センサー IP アドレス 10.0.0.51、IDS ユーザ名 Sensor_user0doc1、および IDS パスワード passowrd01 で侵入検知システムを設定する例を示します。

```
(Cisco Controller) > config wps cids-sensor add 1 10.0.0.51 Sensor_user0doc1 password01
```

関連コマンド

show wps cids-sensor detail

config wps client-exclusion

クライアント除外ポリシーを設定するには、**config wps client-exclusion** コマンドを使用します。

config wps client-exclusion {**802.11-assoc** | **802.11-auth** | **802.11x-auth** | **ip-theft** | **web-auth** | **all**} {**enable** | **disable**}

構文の説明

802.11-assoc	コントローラが 802.11 アソシエーションに連続5回失敗すると、6回目の試行を除外することを指定します。
802.11-auth	コントローラが 802.11 認証に連続 5 回失敗すると、6回目の試行を除外することを指定します。
802.1x-auth	コントローラが 802.11X 認証に連続 5 回失敗すると、6回目の試行を除外することを指定します。
ip-theft	IP アドレスがすでに別のデバイスに割り当てられている場合は、コントローラがクライアントを除外することを指定します。
web-auth	コントローラが Web 認証に連続 3 回失敗すると、4 回目の試行を除外することを指定します。
all	コントローラが上記のすべての理由でクライアントを除外することを指定します。
enable	クライアント除外ポリシーを有効にします。
disable	クライアント除外ポリシーを無効にします。

コマンド デフォルト

すべてのポリシーが有効になります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11 アソシエーションに連続 5 回失敗した場合にクライアントを無効にする例を示します。

```
(Cisco Controller) > config wps client-exclusion 802.11-assoc disable
```

関連コマンド **show wps summary**

config wps mfp

管理フレーム保護（MFP）を設定するには、**config wps mfp** コマンドを使用します。

config wps mfp {**infrastructure** | **ap-impersonation**} {**enable** | **disable**}

構文の説明

infrastructure	MFP インフラストラクチャを設定します。
ap-impersonation	MFP で AP 偽装検出を設定します。
enable	MFP 機能を有効にします。
disable	MFP 機能を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、インフラストラクチャ MFP を有効にする例を示します。

```
(Cisco Controller) > config wps mfp infrastructure enable
```

関連コマンド

show wps mfp

config wps shun-list re-sync

回避リストのコントローラをモビリティ グループ内の他のコントローラと同期させるには、**config wps shun-list re-sync** コマンドを使用します。

config wps shun-list re-sync

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、回避リストのコントローラを他のコントローラと同期するように設定する例を示します。

```
(Cisco Controller) > config wps shun-list re-sync
```

関連コマンド

show wps shun-list

config wps signature

侵入検知システム（IDS）シグニチャ処理を有効または無効にする、または、特定の IDS シグニチャを有効または無効にするには、**config wps signature** コマンドを使用します。

config wps signature {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

構文の説明

standard	標準の IDS シグニチャを設定します。
custom	標準の IDS シグニチャを設定します。
state	IDS シグニチャの状態を指定します。
signature_id	有効または無効にするシグニチャの ID。
enable	IDS シグニチャ処理または特定の IDS シグニチャを有効にします。
disable	IDS シグニチャ処理または特定の IDS シグニチャを無効にします。

コマンド デフォルト

IDS シグニチャ処理は、デフォルトで有効になります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、すべての IDS シグニチャの処理が有効になるように、IDS シグニチャ処理を有効にする例を示します。

```
(Cisco Controller) >config wps signature enable
```

次に、標準の個別の IDS シグニチャを無効にする例を示します。

```
(Cisco Controller) > config wps signature standard state 15 disable
```

関連コマンド

config wps signature frequency

config wps signature interval

config wps signature mac-frequency

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature frequency

個々のアクセス ポイント レベルで特定されるべき、1 間隔あたりの一致パケット数を指定するには、**config wps signature frequency** コマンドを入力します。この値に達すると攻撃が検出されたと判断されます。

config wps signature frequency *signature_id frequency*

構文の説明

signature_id	設定するシグニチャの ID。
frequency	各アクセス ポイント レベルで、攻撃と見なされるまでに識別される必要のある間隔あたりの一致パケット数。範囲は間隔あたり 1 ～ 32,000 パケットです。

コマンド デフォルト

frequency デフォルト値は、シグニチャごとに異なります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、シグニチャ ID 4 に対して、各アクセス ポイントで攻撃と見なされる、間隔あたりの一致パケット数を 1800 に設定する例を示します。

```
(Cisco Controller) > config wps signature frequency 4 1800
```

関連コマンド

config wps signature frequency

config wps signature interval

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature interval

シグニチャ頻度が設定された間隔内でしきい値に達するまでの経過時間（秒数）を指定するには、**config wps signature interval** コマンドを入力します。

config wps signature interval *signature_id interval*

構文の説明

signature_id	設定するシグニチャの ID。
interval	シグニチャの頻度しきい値に達するまでに経過する必要のある秒数。値の範囲は 1 ～ 3,600 秒です。

コマンド デフォルト

interval のデフォルト値は、シグニチャごとに異なります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、シグニチャ ID 1 に対して、シグニチャの頻度しきい値に達するまでに経過する秒数を 200 秒に設定する例を示します。

```
(Cisco Controller) > config wps signature interval 1 200
```

関連コマンド

config wps signature frequency

config wps signature

config wps signature mac-frequency

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature mac-frequency

個々のアクセスポイントでクライアント別に特定されるべき、1間隔あたりの一致パケット数を指定するには、**config wps signature mac-frequency** コマンドを入力します。この値に達すると攻撃が検出されたと判断されます。

config wps signature mac-frequency *signature_id mac_frequency*

構文の説明

signature_id	設定するシグニチャの ID。
mac_frequency	各クライアントおよびアクセス ポイントで、攻撃と見なされる間隔あたりの一致パケット数。範囲は間隔あたり 1 ～ 32,000 パケットです。

コマンド デフォルト

mac_frequency デフォルト値は、シグニチャごとに異なります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、シグニチャ ID 3 に対して、各クライアントで攻撃と見なされる、間隔あたりの一致パケット数を 50 に設定する例を示します。

```
(Cisco Controller) > config wps signature mac-frequency 3 50
```

関連コマンド

config wps signature frequency

config wps signature interval

config wps signature

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature quiet-time

各アクセス ポイントで攻撃が検出されず、アラームが停止するまでの時間の長さを指定するには、**config wps signature quiet-time** コマンドを使用します。

config wps signature quiet-time *signature_id quiet_time*

構文の説明

signature_id	設定するシグニチャの ID。
quiet_time	各アクセス ポイント レベルで攻撃が検出されず、アラームが停止するまでの時間の長さ。値の範囲は 60 ～ 32,000 秒です。

コマンド デフォルト

quiet_time のデフォルト値は、シグニチャごとに異なります。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、シグニチャ ID 1 に対して、アクセス ポイントごとに攻撃が検出されなかったとする経過秒数を 60 秒に設定する例を示します。

```
(Cisco Controller) > config wps signature quiet-time 1 60
```

関連コマンド

config wps signature

config wps signature frequency

config wps signature interval

config wps signature mac-frequency

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature reset

特定の侵入検知システム（IDS）シグニチャまたはすべての IDS シグニチャをデフォルト値にリセットするには、**config wps signature reset** コマンドを使用します。

config wps signature reset {*signature_id* | **all**}

構文の説明

signature_id	リセットする特定の IDS シグニチャの ID。
all	すべての IDS シグニチャをリセットします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、IDS シグニチャ 1 をデフォルト値にリセットする例を示します。

```
(Cisco Controller) > config wps signature reset 1
```

関連コマンド

config wps signature

config wps signature frequency

config wps signature interval

config wps signature mac-frequency

config wps signature quiet-time

show wps signature events

show wps signature summary

show wps summary

第 IV 部

debug コマンド

- debug コマンド：802.11 （1243 ページ）
- debug コマンド：a ～ i （1251 ページ）
- debug コマンド：j ～ q （1317 ページ）
- debug コマンド：r ～ z （1343 ページ）

debug コマンド：802.11

- debug 11k （1244 ページ）
- debug 11w-pmf （1245 ページ）
- debug 11v all （1246 ページ）
- debug 11v detail （1247 ページ）
- debug 11v error （1248 ページ）
- debug 11w-pmf （1249 ページ）

debug 11k

802.11k 設定のデバッグを設定するには、**debug 11k** コマンドを使用します。

debug 11k {**all** | **detail** | **errors** | **events** | **history** | **optimization** | **simulation**} {**enable** | **disable**}

構文の説明

all	すべての 802.11k メッセージのデバッグを設定します。
detail	802.11k 詳細のデバッグを設定します。
errors	802.11k エラーのデバッグを設定します。
events	すべての 802.11k イベントのデバッグを設定します。
history	すべての 802.11k 履歴のデバッグを設定します。Cisco WLC はクライアントのローミング履歴を収集します。
optimization	802.11k 最適化のデバッグを設定します。ネイバー リストの最適化ステップを確認できます。
simulation	802.11k シミュレーション データのデバッグを設定します。クライアント ローミング パラメータの詳細を表示し、オフラインのシミュレーションでのインポートを行うことができます。
enable	802.1k デバッグを有効にします。
disable	802.1k デバッグを無効にします。

コマンド デフォルト

なし。

次に 802.11k シミュレーション データのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug 11k simulation enable
```

関連コマンド

config assisted-roaming

config wlan assisted-roaming

show assisted-roaming

debug 11w-pmf

802.11w のデバッグを設定するには、**debug 11w-pmf** コマンドを使用します。

debug 11w-pmf {**all** | **events** | **keys**} {**enable** | **disable**}

構文の説明

all	すべての 802.11w メッセージのデバッグを設定します。
keys	802.11w キーのデバッグを設定します。
events	802.11w イベントのデバッグを設定します。
enable	802.1w オプションのデバッグを有効にします。
disable	802.1w オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11w キーのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug 11w-pmf keys enable
```

debug 11v all

802.11v デバッグ オプションを設定するには、**debug 11v all** コマンドを使用します。

debug 11v all {**enable | disable**}

構文の説明

enable	すべてのデバッグを有効にします。
disable	すべてのデバッグを無効にします。

コマンド デフォルト

なし

次に、すべてのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug 11v all enable
```

debug 11v detail

802.11v デバッグ詳細を設定するには、**debug 11v detail** コマンドを使用します。

debug 11v detail {**enable | disable**}

構文の説明

enable	デバッグの詳細を有効にします。
disable	デバッグの詳細を無効にします。

コマンド デフォルト

なし

次に、802.11v デバッグ詳細を有効にする例を示します。

```
(Cisco Controller) >debug 11v detail enable
```

debug 11v error

802.11vエラーデバッグ オプションを設定するには、**debug 11v errors** コマンドを使用します。

debug 11v errors {**enable | disable**}

構文の説明

enable	エラーデバッグを有効にします。
disable	エラーデバッグを無効にします。

コマンド デフォルト

なし

次に、802.11v エラー デバッグを有効にする例を示します。

```
(Cisco Controller) >debug 11v error enable
```

debug 11w-pmf

802.11w のデバッグを設定するには、**debug 11w-pmf** コマンドを使用します。

debug 11w-pmf {**all** | **events** | **keys**} {**enable** | **disable**}

構文の説明

all	すべての 802.11w メッセージのデバッグを設定します。
keys	802.11w キーのデバッグを設定します。
events	802.11w イベントのデバッグを設定します。
enable	802.1w オプションのデバッグを有効にします。
disable	802.1w オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11w キーのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug 11w-pmf keys enable
```

debug コマンド：a ～ i

- debug aaa （1253 ページ）
- debug aaa events （1255 ページ）
- debug aaa local-auth （1256 ページ）
- debug airewave-director （1258 ページ）
- debug ap （1260 ページ）
- debug ap enable （1262 ページ）
- debug ap packet-dump （1263 ページ）
- debug ap show stats （1264 ページ）
- debug ap show stats video （1266 ページ）
- debug arp （1267 ページ）
- debug avc （1268 ページ）
- debug bcast （1269 ページ）
- debug call-control （1270 ページ）
- debug capwap （1271 ページ）
- debug capwap reap （1272 ページ）
- debug ccxdiag （1273 ページ）
- debug ccxrm （1274 ページ）
- debug ccxs69 （1275 ページ）
- debug cckm （1276 ページ）
- debug client （1277 ページ）
- debug cts sxp （1278 ページ）
- debug cac （1279 ページ）
- debug cdp （1281 ページ）
- debug crypto （1282 ページ）
- debug dhcp （1283 ページ）
- debug dhcp service-port （1284 ページ）
- debug disable-all （1285 ページ）
- debug dns （1286 ページ）
- debug dot11 （1287 ページ）

- debug dot11 （1288 ページ）
- debug dot11 mgmt interface （1289 ページ）
- debug dot11 mgmt msg （1290 ページ）
- debug dot11 mgmt ssid （1291 ページ）
- debug dot11 mgmt state-machine （1292 ページ）
- debug dot11 mgmt station （1293 ページ）
- debug dot1x （1294 ページ）
- debug dtls （1295 ページ）
- debug fastpath （1296 ページ）
- debug flexconnect avc （1302 ページ）
- debug flexconnect aaa （1303 ページ）
- debug flexconnect acl （1304 ページ）
- debug flexconnect cckm （1305 ページ）
- debug group （1306 ページ）
- debug fmchs （1307 ページ）
- debug flexconnect client ap （1308 ページ）
- debug flexconnect client ap syslog （1309 ページ）
- debug flexconnect client group （1310 ページ）
- debug flexconnect client group syslog （1311 ページ）
- debug flexconnect group （1312 ページ）
- debug ft （1313 ページ）
- debug hotspot （1314 ページ）
- debug ipv6 （1315 ページ）

debug aaa

AAA の設定のデバッグを設定するには、**debug aaa** コマンドを使用します。

debug aaa {[**all** | **avp-xml** | **detail** | **events** | **packet** | **ldap** | **local-auth** | **tacacs**] [**enable** | **disable**]}

構文の説明

all	（任意）すべての AAA メッセージのデバッグを設定します。
avp-xml	（任意）AAA Avp xml イベントのデバッグを設定します。
detail	（任意）AAA エラーのデバッグを設定します。
events	（任意）AAA イベントのデバッグを設定します。
packet	（任意）AAA パケットのデバッグを設定します。
ldap	（任意）AAA Lightweight Directory Access Protocol（LDAP）イベントのデバッグを設定します。
local-auth	（任意）AAA ローカル拡張認証プロトコル（EAP）イベントのデバッグを設定します。
tacacs	（任意）AAA TACACS+ イベントのデバッグを設定します。
enable	（任意）デバッグを有効にします。
disable	（任意）デバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、AAA LDAP イベントのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug aaa ldap enable
```

関連コマンド

debug aaa local-auth eap

show running-config

debug aaa events

DNS ベースの ACL に関連するデバッグを設定するには、**debug aaa events enable** コマンドを使用します。

debug aaa events enable

構文の説明

events	DNS ベースの ACL のデバッグを設定します。

コマンド履歴

リリース	変更内容
7.6	このコマンドが追加されました。

次に、DNS ベースの ACL のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug aaa events enble
```

debug aaa local-auth

Cisco WLC で AAA ローカル認証のデバッグを設定するには、**debug aaa local-auth** コマンドを使用します。

debug aaa local-auth {**db** | **shim** | **eap** {**framework** | **method**} {**all** | **errors** | **events** | **packets** | **sm**}} {**enable** | **disable**}

構文の説明

db	AAA ローカル認証バックエンド メッセージおよびイベントのデバッグを設定します。
shim	AAA ローカル認証シム レイヤ イベントのデバッグを設定します。
eap	AAA ローカル拡張認証プロトコル（EAP）認証のデバッグを設定します。
framework	ローカル EAP フレームワークのデバッグを設定します。
method	ローカル EAP 方式のデバッグを設定します。
all	ローカル EAP メッセージのデバッグを設定します。
errors	ローカル EAP エラーのデバッグを設定します。
events	ローカル EAP イベントのデバッグを設定します。
packets	ローカル EAP パケットのデバッグを設定します。
sm	ローカル EAP ステートマシンのデバッグを指定します。
enable	デバッグを開始します。
disable	デバッグを終了します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、AAA ローカル EAP 認証のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug aaa local-auth eap method all enable
```

関連コマンド

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

show local-auth certificates

show local-auth config

show local-auth statistics

debug airewave-director

Airewave Director ソフトウェアのデバッグを設定するには、**debug airwave-director** コマンドを使用します。

debug airewave-director {**all** | **channel** | **detail** | **error** | **group** | **manager** | **message** | **packet** | **power** | **profile** | **radar** | **rf-change**} {**enable** | **disable**}

構文の説明

all	すべての Airewave Director ログのデバッグを設定します。
channel	Airewave Director チャネル割り当てプロトコルのデバッグを設定します。
detail	Airewave Director 詳細ログのデバッグを設定します。
error	Airewave Director エラー ログのデバッグを設定します。
group	Airewave Director グループ化プロトコルのデバッグを設定します。
manager	Airewave Director マネージャのデバッグを設定します。
message	Airewave Director メッセージのデバッグを設定します。
packet	Airewave Director パケットのデバッグを設定します。
power	Airewave Director 電力割り当てプロトコルおよびカバレッジ ホール検出のデバッグを設定します。
profile	Airewave Director プロファイル イベントのデバッグを設定します。
radar	Airewave Director レーダー検出/回避プロトコルのデバッグを設定します。
rf-change	Airewave Director rf 変更のデバッグを設定します。
enable	Airewave Director のデバッグを有効にします。
disable	Airewave Director のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Airewave Director プロファイルイベントのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug airewave-director profile enable
```

関連コマンド

debug disable-all

show sysinfo

debug ap

Cisco Lightweight アクセス ポイントのリモート デバッグを設定したり、Lightweight アクセス ポイントでコマンドをリモートで実行したりするには、**debug ap** コマンドを使用します。

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

構文の説明

enable	Lightweight アクセス ポイント上でのデバッグを有効にします。 （注） デバッグ情報はコントローラのコンソール上だけに表示され、コントローラの Telnet/SSH CLI セッションに出力は送信されません。
disable	Lightweight アクセス ポイント上でのデバッグを無効にします。 （注） デバッグ情報はコントローラのコンソール上だけに表示され、コントローラの Telnet/SSH CLI セッションに出力は送信されません。
command	アクセス ポイントで CLI コマンドが実行されることを指定します。
cmd	実行するコマンド。 （注） 実行するコマンドは、二重引用符で囲む必要があります（例：**debug ap command “led flash 30” AP03**）。 コマンドの出力はコントローラのコンソール上だけに表示され、コントローラの Telnet/SSH CLI セッションに出力は送信されません。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのリモート デバッグは無効です。

次に、アクセス ポイント AP01 でリモート デバッグを有効にする例を示します。

```
(Cisco Controller) >debug ap enable AP01
```

次に、アクセス ポイント AP02 で **config ap location** コマンドを実行する例を示します。

```
(Cisco Controller) >debug ap command “config ap location "Building 1" AP02”
```

次に、アクセス ポイント AP03 でフラッシュ LED コマンドを実行する例を示します。

```
(Cisco Controller) >debug ap command “led flash 30” AP03
```

debug ap enable

Cisco Lightweight アクセス ポイントのリモート デバッグを設定したり、Lightweight アクセス ポイントでコマンドをリモートで実行したりするには、**debug ap enable** コマンドを使用します。

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

構文の説明

enable	リモート デバッグを有効にします。 （注） デバッグ情報はコントローラのコンソール上だけに表示され、コントローラの Telnet/SSH CLI セッションに出力は送信されません。
disable	リモート デバッグを無効にします。
command	アクセス ポイントで CLI コマンドが実行されることを指定します。
cmd	実行するコマンド。 （注） 実行するコマンドは、二重引用符で囲む必要があります（例：**debug ap command “led flash 30” AP03**）。 コマンドの出力はコントローラのコンソール上だけに表示され、コントローラの Telnet/SSH CLI セッションに出力は送信されません。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、アクセス ポイント AP01 でリモート デバッグを有効にする例を示します。

```
(Cisco Controller) >debug ap enable AP01
```

次に、アクセス ポイント AP02 でリモート デバッグを無効にする例を示します。

```
(Cisco Controller) >debug ap disable AP02
```

次に、アクセス ポイント AP03 でフラッシュ LED コマンドを実行する例を示します。

```
(Cisco Controller) >debug ap command "led flash 30" AP03
```

debug ap packet-dump

パケット キャプチャのデバッグを設定するには、**debug ap packet-dump** コマンドを使用します。

debug ap packet-dump {**enable** | **disable**}

構文の説明

enable	アクセス ポイントのパケット キャプチャのデバッグを有効にします。
disable	アクセス ポイントのパケット キャプチャのデバッグを無効にします。

コマンド デフォルト

パケット キャプチャのデバッグは無効です。

使用上のガイドライン

Cisco WLC 間ローミング中には、パケット キャプチャは機能しません。

Cisco WLC では、ビーコンやプローブの応答など、無線ファームウェアに作成され、アクセス ポイントから送信されたパケットをキャプチャしません。Tx パスで無線ドライバを通過するパケットだけがキャプチャされます。

次に、アクセス ポイントからのパケット キャプチャのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug ap packet-dump enable
```

debug ap show stats

Cisco Lightweight アクセス ポイントのビデオ メッセージおよび統計情報のトラブルシューティングを行うには、**debug ap show stats** コマンドを使用します。

debug ap show stats {**802.11a** | **802.11b**} *cisco_ap* {**tx-queue** | **packet** | **load** | **multicast** | **client** {*client_MAC* | **video** | **all**} | **video metrics**}

debug ap show stats video *cisco_ap* {**multicast mgid** *mgid_database_number* | **admission** | **bandwidth**}

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b/g ネットワークを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
tx-queue	AP の送信キューのトラフィック統計情報を表示します。
packet	AP のパケット統計情報を表示します。
load	AP の QoS Basic Service Set（QBSS）とその他の統計情報を表示します。
multicast	AP のマルチキャスト サポート対象レート統計情報を表示します。
client	指定されたクライアントのメトリック統計情報を表示します。
client_MAC	クライアントの MAC アドレス。
video	AP のすべてのクライアントのビデオ統計情報を表示します。
all	AP のすべてのクライアントの統計情報を表示します。
video metrics	ビデオ メトリック統計情報を表示します。
mgid	単一マルチキャスト グループ ID（MGID）の詳細なマルチキャスト情報を表示します。
mgid_database_number	レイヤ 2 MGID データベース番号。
admission	AP のビデオ アドミッション制御を表示します。

bandwidth	AP のビデオ帯域幅を表示します。

コマンド デフォルト なし

次に、802.11a ネットワーク上でアクセス ポイント AP01 送信キュー トラフィックのトラブルシューティングを行う例を示します。

```
(Cisco Controller) >debug ap show stats 802.11a AP01 tx-queue
```

次に、802.11b/g ネットワーク上でアクセス ポイント AP02 マルチキャスト サポート対象レートのトラブルシューティングを行う例を示します。

```
(Cisco Controller) >debug ap show stats 802.11b AP02 multicast
```

次に、802.11a ネットワーク上で、アクセス ポイント AP01 とアソシエートされている MAC アドレスで識別されるクライアントのメトリックのトラブルシューティングを行う例を示します。

```
(Cisco Controller) >debug ap show stats 802.11a AP01 client 00:40:96:a8:f7:98
```

次に、802.11a ネットワーク上で、アクセス ポイント AP01 とアソシエートされているすべてのクライアントのメトリックのトラブルシューティングを行う例を示します。

```
(Cisco Controller) >debug ap show stats 802.11a AP01 client all
```

debug ap show stats video

Cisco Lightweight アクセス ポイントのビデオ メッセージおよび統計情報のデバッグを設定するには、**debug ap show stats video** コマンドを使用します。

debug ap show stats video *cisco_ap* {**multicast mgid** *mgid_value* | **admission** | **bandwidth**}

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイント名。
multicast mgid	アクセス ポイントの指定 MGID に対するマルチキャスト データベース関連情報を表示します。
mgid_value	1 ～ 4095 のレイヤ 2 MGID データベース番号。
admission	ビデオ アドミッション制御を表示します。
bandwidth	ビデオ帯域幅を表示します。

コマンド デフォルト

なし

次に、グループのレイヤ 2 MGID データベース番号で識別されたアクセス ポイント AP01 のマルチキャスト グループのデバッグを設定する例を示します。

```
(Cisco Controller) >debug ap show stats video AP01 multicast mgid 50
```

次に、アクセス ポイント AP01 のビデオ帯域幅のデバッグを設定する例を示します。

```
(Cisco Controller) >debug ap show stats video AP01 bandwidth
```

debug arp

Address Resolution Protocol（ARP）オプションのデバッグを設定するには、**debug arp** コマンドを使用します。

debug arp {**all** | **detail** | **events** | **message**} {**enable** | **disable**}

構文の説明

all	すべての ARP ログのデバッグを設定します。
detail	ARP の詳細メッセージのデバッグを設定します。
error	ARP エラーのデバッグを設定します。
message	ARP メッセージのデバッグを設定します。
enable	ARP デバッグを有効にします。
disable	ARP デバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ARP デバッグ設定を有効にする例を示します。

```
(Cisco Controller) > debug arp error enable
```

次に、ARP デバッグ設定を無効にする例を示します。

```
(Cisco Controller) > debug arp error disable
```

関連コマンド

debug disable-all

show sysinfo

debug avc

Application Visibility and Control（AVC）オプションのデバッグを設定するには、**debug avc error** コマンドを使用します。

debug avc {**events** | **error**} {**enable** | **disable**}

構文の説明

events	AVC イベントのデバッグを設定します。
error	AVC エラーのデバッグを設定します。
enable	AVCイベントまたはエラーのデバッグを有効にします。
disable	AVCイベントまたはエラーのデバッグを無効にします。

コマンド デフォルト

デフォルトでは、AVC オプションのデバッグは無効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、AVC エラーのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug avc error enable
```

関連コマンド

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug bcast

ブロードキャスト オプションのデバッグを設定するには、**debug bcast** コマンドを使用します。

debug bcast {**all** | **error** | **message** | **igmp** | **detail**} {**enable** | **disable**}

構文の説明

all	すべてのブロードキャスト ログのデバッグを設定します。
error	ブロードキャスト エラーのデバッグを設定します。
message	ブロードキャスト メッセージのデバッグを設定します。
igmp	ブロードキャスト IGMP メッセージのデバッグを設定します。
detail	ブロードキャスト詳細メッセージのデバッグを設定します。
enable	ブロードキャスト デバッグを有効にします。
disable	ブロードキャスト デバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ブロードキャスト メッセージに対するデバッグを有効にする例を示します。

```
(Cisco Controller) > debug bcast message enable
```

次に、ブロードキャスト メッセージに対するデバッグを無効にする例を示します。

```
(Cisco Controller) > debug bcast message disable
```

関連コマンド

debug disable-all

show sysinfo

debug call-control

SIP コール制御設定に対するデバッグを設定するには、**debug call-control** コマンドを使用します。

debug call-control {**all** | **event**} {**enable** | **disable**}

構文の説明

all	すべての SIP コール制御メッセージに対するデバッグ オプションを設定します。
event	SIP コール制御イベントに対するデバッグ オプションを設定します。
enable	SIP コール制御メッセージまたはイベントのデバッグを有効にします。
disable	SIP コール制御メッセージまたはイベントのデバッグを無効にします。

コマンド デフォルト

ディセーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての SIP コール制御メッセージのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug call-control all enable
```

debug capwap

Control and Provisioning of Wireless Access Points（CAPWAP）設定のデバッグを設定するには、**debug capwap** コマンドを使用します。

debug capwap {**detail** | **dtls-keepalive** | **errors** | **events** | **hexdump** | **info** | **packet** | **payload** | **mfp**} {**enable** | **disable**}

構文の説明

detail	CAPWAP の詳細設定のデバッグを設定します。
dtls-keepalive	CAPWAP DTLS データ キープアライブ パケット設定のデバッグを設定します。
errors	CAPWAP エラー設定のデバッグを設定します。
events	CAPWAP イベント設定のデバッグを設定します。
hexdump	CAPWAP 16進数ダンプ設定のデバッグを設定します。
info	CAPWAP 情報設定のデバッグを設定します。
packet	CAPWAP パケットの設定のデバッグを設定します。
payload	CAPWAP ペイロード設定のデバッグを設定します。
mfp	CAPWAP mfp 設定のデバッグを設定します。
enable	CAPWAP のコマンドのデバッグを有効にします。
disable	CAPWAP のコマンドのデバッグを無効にします。

コマンド デフォルト

なし

次に、CAPWAP の詳細のデバッグを有効にする例を示します。

```
(Cisco Controller) >debug capwap detail enable
```

debug capwap reap

FlexConnect アクセス ポイントにおける Control and Provisioning of Wireless Access Points（CAPWAP）設定のデバッグを設定するには、**debug capwap reap** コマンドを使用します。

debug capwap reap ［**mgmt** | **load**］

構文の説明

mgmt	（任意）クライアント認証と関連メッセージのデバッグを設定します。
load	（任意）ペイロード アクティビティのデバッグを設定します。FlexConnect アクセス ポイントをスタンドアロン モードで起動する場合に便利です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect クライアント認証および関連メッセージのデバッグを設定する例を示します。

```
(Cisco Controller) >debug capwap reap mgmt
```

debug ccxdiag

Cisco Compatible Extensions（CCX）診断オプションのデバッグを設定するには、**debug ccxdiag** コマンドを使用します。

debug ccxdiag {**all** | **error** | **event** | **packet**} {**enable** | **disable**}

構文の説明

all	すべてのCCX S69メッセージのデバッグを設定します。
error	CCX S69 エラーのデバッグを設定します。
event	CCX S69 イベントのデバッグを設定します。
packet	CCX S69 パケットのデバッグを設定します。
enable	CCX S69 オプションのデバッグを有効にします。
disable	CCX S69 オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CCX S69 パケットのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug ccxdiag packets enable
```

debug ccxrm

CCX Cisco Client Extension（CCX）無線管理（RM）のデバッグを設定するには、**debug ccxrm** コマンドを使用します。

debug ccxrm {**all** | **detail** | **error** | **location-calibration** | **message** | **packet** | **warning**} {**enable** | **disable**}

構文の説明

all	すべての CCX RM メッセージのデバッグを設定します。
detail	CCX RM の詳細デバッグを設定します。
error	CCX RM エラーのデバッグを設定します。
location-calibration	CCX RM ロケーション キャリブレーションのデバッグを設定します。
message	CCX RM メッセージのデバッグを設定します。
packet	CCX RM パケットのデバッグを設定します。
warning	CCX RM 警告のデバッグを設定します。
enable	CCX RM オプションのデバッグを有効にします。
disable	CCX RM オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CCX RM のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug ccxrm all enable
```

debug ccxs69

CCX S69 タスクのデバッグを設定するには、**debug ccxs69** コマンドを使用します。

debug ccxs69 {**all** | **error** | **event**} {**enable**| **disable**}

構文の説明

all	すべての CCX S69 メッセージのデバッグを設定します。
error	CCX S69 エラーのデバッグを設定します。
event	CCX S69 イベントのデバッグを設定します。
enable	CCX S69 オプションのデバッグを有効にします。
disable	CCX S69 オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CCX S69 のデバッグを有効にする例を示します。

```
(Cisco Controller) >debug ccxs69 all enable
```

debug cckm

Cisco Centralized Key Management オプションのデバッグを設定するには、次のコマンドを使用します： **debug cckm**

debug cckm {**client** | **detailed**} {**enable**| **disable**}

構文の説明

client	クライアントの Cisco Centralized Key Management のデバッグを設定します。
detailed	Cisco Centralized Key Management の詳細デバッグを設定します。
enable	Cisco Centralized Key Management のデバッグを有効にします。
disable	Cisco Centralized Key Management のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CiscoCentralized Key Management の詳細デバッグを有効にする例を示します。

```
(Cisco Controller) > debug cckm detailed enable
```

debug client

特定のクライアントのデバッグを設定するには、**debug client** コマンドを使用します。

debug client *mac_address*

構文の説明

mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

使用上のガイドライン

debug client *mac_address* コマンドの入力後に **debug aaa events enable** コマンドを入力すると、その特定のクライアント MAC アドレスの AAA イベント ログが表示されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。

次に、特定のクライアントをデバッグする場合の設定例を示します。

```
(Cisco Controller) > debug client 01:35:6x:yy:21:00
```

debug cts sxp

Cisco TrustSec SXP オプションのデバッグを設定するには、**debug cts sxp** コマンドを使用します。

debug cts sxp {**all** | **errors** | **events** | **framework** | **message**} {**enable** | **disable**}

構文の説明

all	すべてのCTS SXPオプションのデバッグを設定します。
errors	CTS SXP エラーのデバッグを設定します。
events	CTS SXP イベントのデバッグを設定します。
framework	CTS SXP フレームワークのデバッグを設定します。
message	CTS SXP メッセージのデバッグを設定します。
enable	デバッグを有効にします。
disable	デバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

debug cac

コール アドミッション制御（CAC）オプションのデバッグを設定するには、**debug cac** コマンドを使用します。

debug cac {**all** | **event** | **packet**} {**enable** | **disable**}

構文の説明

all	すべてのCACメッセージにデバッグ オプションを設定します。
event	CACイベントにデバッグ オプションを設定します。
packet	選択した CAC パケットにデバッグ オプションを設定します。
kts	KTS ベースの CAC メッセージにデバッグ オプションを設定します。
enable	CAC 設定のデバッグを有効にします。
disable	CAC 設定のデバッグを無効にします。

コマンド デフォルト

デフォルトでは、CAC オプションのデバッグは無効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CAC 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug cac event enable
(Cisco Controller) > debug cac packet enable
```

関連コマンド

config 802.11 cac video acm

config 802.11 cac video max-bandwidth

config 802.11 video roam-bandwidth

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac voice load-based

config 802.11 cac voice roam-bandwidth

config 802.11cac voice stream-size

config 802.11cac voice tspec-inactivity-timeout

debug cdp

CDP のデバッグを設定するには、**debug cdp** コマンドを使用します。

debug cdp {**events** | **packets**} {**enable** | **disable**}

構文の説明

events	CDP イベントのデバッグを設定します。
packets	CDP パケットのデバッグを設定します。
enable	CDP オプションのデバッグを有効にします。
disable	CDP オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco コントローラで CDP イベントのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug cdp
```

debug crypto

ハードウェア暗号オプションのデバッグを設定するには、**debug crypto** コマンドを使用します。

debug crypto {**all** | **sessions** | **trace** | **warning**} {**enable** | **disable**}

構文の説明

all	すべてのハードウェア クリプト メッセージのデバッグを設定します。
sessions	ハードウェア クリプト セッションのデバッグを設定します。
trace	ハードウェア クリプト セッションのデバッグを設定します。
warning	ハードウェア クリプト セッションのデバッグを設定します。
enable	ハードウェア暗号セッションのデバッグを有効にします。
disable	ハードウェア暗号セッションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ハードウェア暗号セッションのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug crypto sessions enable
```

関連コマンド

debug disable-all

show sysinfo

debug dhcp

DHCP のデバッグを設定するには、**debug dhcp** コマンドを使用します。

debug dhcp {**message** | **packet**} {**enable** | **disable**}

構文の説明

message	DHCP エラー メッセージのデバッグを設定します。
packet	DHCP パケットのデバッグを設定します。
enable	DHCP メッセージまたはパケットのデバッグを有効にします。
disable	DHCP メッセージまたはパケットのデバッグを無効にします。

コマンド デフォルト

なし

次に、DHCP メッセージのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug dhcp message enable
```

debug dhcp service-port

サービス ポートでの Dynamic Host Configuration Protocol（DHCP）パケットのデバッグを有効または無効にするには、**debug dhcp service-port** コマンドを使用します。

debug dhcp service-port {**enable** | **disable**}

構文の説明

enable	サービス ポートでの DHCP パケットのデバッグをイネーブルにします。
disable	サービス ポートでの DHCP パケットのデバッグをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、サービス ポートでの DHCP パケットのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug dhcp service-port enable
```

debug disable-all

すべてのデバッグ メッセージを無効にするには、**debug disable-all** コマンドを使用します。

debug disable-all

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのデバッグ メッセージを無効にする例を示します。

```
(Cisco Controller) > debug disable-all
```

debug dns

ドメイン ネーム システム（DNS） オプションのデバッグを設定するには、**debug dns** コマンドを使用します。

debug dns {**all** | **detail** | **error** | **message**} {**enable** | **disable**}

構文の説明

all	すべてのDNSオプションのデバッグを設定します。
detail	DNS 詳細のデバッグを設定します。
error	DNS エラーのデバッグを設定します。
message	DNS メッセージのデバッグを設定します。
enable	DNS オプションのデバッグを有効にします。
disable	DNS オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、DNS エラーのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug dns error enable
```

debug dot11

802.11 イベントのデバッグを設定するには、**debug dot11** コマンドを使用します。

debug dot11 {**all** | **load-balancing** | **management** | **mobile** | **nmsp** | **probe** | **rldp** | **rogue** | **state**} {**enable** | **disable**}

構文の説明

all	すべての 802.11 メッセージのデバッグを設定します。
load-balancing	802.11 ロード バランシング イベントのデバッグを設定します。
management	802.11 MAC 管理メッセージのデバッグを設定します。
mobile	802.11 のモバイル イベントのデバッグを設定します。
nmsp	802.11 NMSP インターフェイス イベントのデバッグを設定します。
probe	プローブのデバッグを設定します。
rldp	802.11 不正位置検出のデバッグを設定します。
rogue	802.11 不正イベントのデバッグを設定します。
state	802.11 モバイル状態遷移のデバッグを設定します。
enable	802.11 のデバッグを有効にします。
disable	802.11 のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug dot11 state enable
(Cisco Controller) > debug dot11 mobile enable
```

debug dot11

802.11 イベントのデバッグを設定するには、**debug dot11** コマンドを使用します。

debug dot11 {**all** | **load-balancing** | **management** | **mobile** | **nmsp** | **probe** | **rldp** | **rogue** | **state**} {**enable** | **disable**}

構文の説明

all	すべての 802.11 メッセージのデバッグを設定します。
load-balancing	802.11 ロードバランシング イベントのデバッグを設定します。
management	802.11 MAC 管理メッセージのデバッグを設定します。
mobile	802.11 のモバイル イベントのデバッグを設定します。
nmsp	802.11 NMSP インターフェイス イベントのデバッグを設定します。
probe	プローブのデバッグを設定します。
rldp	802.11 不正位置検出のデバッグを設定します。
rogue	802.11 不正イベントのデバッグを設定します。
state	802.11 モバイル状態遷移のデバッグを設定します。
enable	802.11 のデバッグを有効にします。
disable	802.11 のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug dot11 state enable
(Cisco Controller) > debug dot11 mobile enable
```

debug dot11 mgmt interface

802.11 管理インターフェイス イベントのデバッグを設定するには、**debug dot11 mgmt interface** コマンドを使用します。

debug dot11 mgmt interface

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11 管理インターフェイス イベントをデバッグする例を示します。

```
(Cisco Controller) >debug dot11 mgmt interface
```

debug dot11 mgmt msg

802.11 管理メッセージのデバッグを設定するには、**debug dot11 mgmt msg** コマンドを使用します。

debug dot11 mgmt msg

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、dot11 管理メッセージを有効にする例を示します。

```
(Cisco Controller) >debug dot11 mgmt msg
```

debug dot11 mgmt ssid

802.11 管理イベントのデバッグを設定するには、**debug dot11 mgmt ssid** コマンドを使用します。

debug dot11 mgmt ssid

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11 SSID 管理イベントのデバッグを設定する例を示します。

```
(Cisco Controller) >debug dot11 mgmt ssid
```

debug dot11 mgmt state-machine

802.11 ステート マシンのデバッグを設定するには、**debug dot11 mgmt state-machine** コマンドを使用します。

debug dot11 mgmt state-machine

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11 ステート マシンのデバッグを設定する例を示します。

```
(Cisco Controller) >debug dot11 mgmt state-machine
```

debug dot11 mgmt station

管理ステーション設定のデバッグを設定するには、**debug dot11 mgmt station** コマンドを使用します。

debug dot11 mgmt station

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、管理ステーション設定のデバッグを設定する例を示します。

```
(Cisco Controller) >debug dot11 mgmt station
```

debug dot1x

802.1X オプションのデバッグを設定するには、**debug dot1x** コマンドを使用します。

debug dot1x {**aaa** | **all** | **events** | **packets** | **states**} {**enable** | **disable**}

構文の説明

aaa	802.1X AAA 相互作用のデバッグを設定します。
all	すべての 802.1X メッセージのデバッグを設定します。
events	802.1X イベントのデバッグを設定します。
packets	802.1X パケットのデバッグを設定します。
states	802.1X 状態遷移のデバッグを設定します。
enable	802.1X オプションのデバッグを有効にします。
disable	802.1X オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.1X 状態遷移のデバッグをイネーブルにする例を示します。

```
(Cisco Controller) > debug dot1x states enable
```

debug dtls

Datagram Transport Layer Security（DTLS） オプションのデバッグを設定するには、**debug dtls** コマンドを使用します。

debug dtls {**all** | **event** | **packet** | **trace**} {**enable** | **disable**}

構文の説明

all	すべてのDTLSメッセージのデバッグを設定します。
event	DTLS イベントのデバッグを設定します。
packet	DTLS パケットのデバッグを設定します。
trace	DTLS トレース メッセージのデバッグを設定します。
enable	DTLS オプションのデバッグを有効にします。
disable	DTLS オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

ここで説明したデバッグ アクションは、CAPWAP トラブルシューティングと組み合わせて使用されます。

次に、DTLS パケット デバッグをイネーブルにする例を示します。

```
(Cisco Controller) > debug dtls packet enable
```

debug fastpath

コントローラの 10 ギガビット イーサネット インターフェイスの問題をデバッグし、コントローラのすべての管理および制御機能の詳細を表示するには、**debug fastpath** コマンドを使用します。

debug fastpath [{**disable**|**enable**|**errors**|**events**|**warning**|**log**|**status**|**dump**|**audit**|**clear**}]
debug fastpath log [{*error events show*}]
debug fastpath dump [{**stats** *DP_number*} | {**fpapool***DP_number*} | {**ownerdb**} | {**portdb**} | {**tun4db***indexDP_number*} | {**scbdb***indexDP_number*} | {**cfgtool -- dump.sfp**} | {**urlacldb***start-acl-id start-rule-index* } | {**vlandb**} | { **dpcp-stats**} | { **clear** *stats*} | {**systemdb**} | {**debug**|{**wlanappstats***wlan_id*}} | { **appqosdb**}]

構文の説明

disable	fastpath メッセージのデバッグを有効にします。
enable	fastpath メッセージのデバッグを無効にします。
errors	fastpath エラーに関連するデバッグ メッセージを表示します。
events	fastpath イベントに関連するデバッグ メッセージを表示します。
warnings	fastpath 警告に関連するデバッグ メッセージを表示します。
log	ログ メッセージのデバッグを設定します。
errors	fastpath エラーのデバッグを設定します。
events	fastpath イベントのデバッグを設定します。
show	fastpath に関連する最新イベントのログを表示します。
status	fastpath 設定のステータスを表示します。
dump	CLI ダンプ コマンドを表示します。
stats	データ プレーンからのデバッグの統計情報を表示します。

DP_number	選択したデータ プレーン番号に基づいて、データ プレーンの統計カウンタを表示します。値には 0、1、[All] が含まれます。デフォルトのオプションは [All] です。次のように選択する必要があります。 • シスコ ワイヤレス LAN コントローラ 2504 シリーズ、シスコ ワイヤレス LAN コントローラ 5508 シリーズ、シスコ ワイヤレス LAN コントローラ 7500 シリーズ、シスコ ワイヤレス LAN コントローラ 8500 シリーズにはインデックス 0。 • WiSM2 の 2 つのデータ プレーンに対して、個々のデータ プレーンまたは両方のデータ プレーンの統計情報を表示するには、それぞれにインデックス 0 または 1 またはその両方。
fpapool	データ プレーンのパケット バッファの統計情報を表示します。
DP_number	データ プレーン番号に基づいてパケット バッファの統計情報を表示します。値には 0、1、[All] が含まれます。デフォルトのオプションは [All] です。次のように選択する必要があります。 • シスコ ワイヤレス LAN コントローラ 2504 シリーズ、シスコ ワイヤレス LAN コントローラ 5508 シリーズ、シスコ ワイヤレス LAN コントローラ 7500 シリーズ、シスコ ワイヤレス LAN コントローラ 8500 シリーズにはインデックス 0。 • WiSM2 の 2 つのデータ プレーンに対して、個々のデータ プレーンまたは両方のデータ プレーンの統計情報を表示するには、それぞれにインデックス 0 または 1 またはその両方。
ownerdb	データ プレーンの所有者情報を表示します。
portdb	データ プレーンのポート データベースを表示します。
tun4db	データ プレーンから最初の 20 トンネルをダンプします。

index	入力されたインデックスから20のトンネルエントリをダンプします。WISM2データプレーンのプロセッサを示すには、データ プレーン番号 0/1 を使用する必要があります。
DP_number	データプレーンから最初の20のクライアントエントリをダンプします。値には0、1、[All]が含まれます。デフォルトのオプションは[All]です。次のように選択する必要があります。 • シスコ ワイヤレスLANコントローラ2504シリーズ、シスコ ワイヤレス LAN コントローラ5508シリーズ、シスコ ワイヤレス LAN コントローラ 7500 シリーズ、シスコ ワイヤレス LAN コントローラ 8500 シリーズにはインデックス 0。 • WiSM2 の 2 つのデータ プレーンに対して、個々のデータ プレーンまたは両方のデータ プレーンの統計情報を表示するには、それぞれにインデックス 0 または 1 またはその両方。
scbdb	入力されたインデックスから始まる20のクライアント エントリをダンプします。WISM2データプレーンのプロセッサを示すには、データ プレーン番号 0/1 を使用する必要があります。
index	選択したMACアドレスのクライアント情報をダンプします。
DP_number	データプレーンから最初の20のクライアントエントリをダンプします。値には0、1、[All]が含まれます。デフォルトのオプションは[All]です。次のように選択する必要があります。 • シスコ ワイヤレスLANコントローラ2504シリーズ、シスコ ワイヤレス LAN コントローラ5508シリーズ、シスコ ワイヤレス LAN コントローラ 7500 シリーズ、シスコ ワイヤレス LAN コントローラ 8500 シリーズにはインデックス 0。 • WiSM2 の 2 つのデータ プレーンに対して、個々のデータ プレーンまたは両方のデータ プレーンの統計情報を表示するには、それぞれにインデックス 0 または 1 またはその両方。

cfgtool -- dump.sfp	SX/LC/T 小型フォーム ファクタ プラグイン（SFP）モジュールのモデル/タイプと OUI 部品番号を表示します。
urlacldb *start-acl-id start-rule-index*	URL ACL データベースをダンプします。
vlandb	データ プレーンの VLAN データベースをダンプします。
dpcp-stats	データ プレーンからコントロール プレーンへのメッセージの統計情報を表示します。
clear stats	データプレーン統計カウンタをクリアします。
systemdb	グローバル データ プレーン設定を表示します。
debug	トラブルシューティングを有効にするため、データ プレーンのいくつかの最新メッセージを表示します。
wlanappstats	WLAN の Application Visibility and Control（AVC）統計情報を表示します。
wlan_id	AVC 統計情報を特定するために必要な WLAN の WLAN ID。
appqosdb	データ プレーンの Application Visibility and Control（AVC）データベース統計情報を表示します。
clear	コマンドをクリアします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.3	このコマンドは、本リリースで強化されました。追加された新しいキーワードは urlacldb です。

使用上のガイドライン

なし

例

次に、SX/LC/T 小型フォーム ファクタ プラグイン（SFP）モジュールのモデル/タイプとそれぞれの OUI 部品番号の例を示します。

```
(Cisco Controller) >debug fastpath status

           STP   Admin    Physical   Physical   Link   Link
Pr  Type   Stat   Mode     Mode      Status   Status  Trap     POE
SFPType
-- ------- ---- ------- ---------- ---------- ------ ------- -------
----------
1  Normal  Forw Enable  Auto       1000 Full  Up     Enable  N/A
1000BaseTX
2  Normal  Forw Enable  Auto       1000 Full  Up     Enable  N/A
1000BaseTX
```

次に、status コマンドの実行中に表示される fastpath ステータスの例を示します。

```
(Cisco Controller) >debug fastpath status

FP0.03:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.00:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.06:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.05:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.06:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.03:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.06:(119115)Received command: FP_CMD_ACL_COUNTER_GET
FP0.07:(119125)Received command: FP_CMD_ACL_COUNTER_GET
FP0.04:(119125)Received command: FP_CMD_ACL_COUNTER_GET
FP0.03:(119125)Received command: FP_CMD_ACL_COUNTER_GET
```

次に、debug fastpath log errors コマンドの実行中に表示される fastpath エラーの例を示します。

```
(Cisco Controller) >debug fastpath log errors

FP0.04:(873365)[fp_ingress_capwap:429]Discarding Control/Data
Plane DTLS-Application packets after Lookup Failed
FP0.02:(873418)Change logDebugLevel from: 0x1e to 0x9
```

次に、debug fastpath log events コマンドの実行中に表示される fastpath イベントの例を示します。

```
(Cisco Controller) >debug fastpath log events

FP0.09:(873796)[fp_ingress_capwap:429]Discarding Control/Dat
a Plane DTLS-Application packets after Lookup Failed
FP0.06:(873921)Change logDebugLevel from: 0x9 to 0x1e
```

次に、debug fastpath log show コマンドの実行中に表示される例を示します。

```
(Cisco Controller) >debug fastpath log show

FP0.07:(874033)Change logDebugLevel from: 0x1e to 0x9
Fastpath CPU0.02: FAST CACHE DISABLED
Fastpath CPU0.02: FAST CACHE ENABLED
Fastpath CPU0.00: Received command: FP_CMD_ADD_AP
Fastpath CPU0.05: Received command: FP_CMD_DEL_TUN4 ifTun=1113
Fastpath CPU0.03: Received command: FP_CMD_DEL_TUN4 ifTun=3161
```

```
Fastpath CPU0.03: Received command: FP_CMD_DEL_AP
FP0.02:[cmdDelMcastRgTun:6733]failed to delete mcast rg tun 0 ifTun=3161
FP0.07:[fp_ingress_capwap:429]Discarding Control/Data Plane
DTLS-Application packets after Lookup Failed
FP0.01:[fp_ingress_capwap:429]Discarding Control/Data Plane
DTLS-Application packets after Lookup Failed
Fastpath CPU0.01: Received command: FP_CMD_ADD_TUN4 type=CAPWAP
ifTun=1114 dstIP
=9.4.110.100 dstMac=2037.06e2.5ec4 dstIPv6=
0000:0000:0000:0000:0000:0000:0000:0000
Fastpath CPU0.01: Tunnel 1114 srcip=9041820 dstip=9046e64
xor=0x7644(30276) LAG Offset=0,0,0,0,1,0,1,4
Fastpath CPU0.09: Received command: FP_CMD_ADD_TUN4 type=CAPWAP
ifTun=3162 dstIP
=9.4.110.100 dstMac=2037.06e2.5ec4 dstIPv6=
0000:0000:0000:0000:0000:0000:0000:0000
Fastpath CPU0.09: Tunnel 3162 srcip=9041820 dstip=9046e64
xor=0x7644(30276) LAG Offset=0,0,0,0,1,0,1,4
Fastpath CPU0.00: Received command: FP_CMD_SET_INTERFACE_MTU
Fastpath CPU0.00: FAST CACHE DISABLED
Fastpath CPU0.00: FAST CACHE ENABLED
Fastpath CPU0.00: Received command: FP_CMD_ADD_AP
Fastpath CPU0.03: Received command: FP_CMD_UPDATE_EOIP for index=5122
Fastpath CPU0.02: Received command: FP_CMD_UPDATE_EOIP for index=5122
Fastpath CPU0.00: Received command: FP_CMD_DEL_TUN4 ifTun=1114
Fastpath CPU0.03: Received command: FP_CMD_DEL_TUN4 ifTun=3162
Fastpath CPU0.03: Received command: FP_CMD_DEL_AP
FP0.04:[cmdDelMcastRgTun:6733]failed to delete mcast rg tun 0 ifTun=3162
```

debug flexconnect avc

Flexconnect Application Visibility and Control（AVC）イベントをデバッグするには、**debug flexconnect avc** コマンドを使用します。

debug flexconnect ave {**event** | **error** | **detail**} {**enable** | **disable**}

構文の説明

event	FlexConnect AVC イベントをデバッグします。
error	FlexConnect AVC エラーをデバッグします。
detail	FlexConnect AVC の詳細をデバッグします。
enable	デバッグを有効にします。
disable	デバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、イベントのデバッグ アクションを有効にする例を示します。

```
(Cisco Controller) >debug flexconnect avc event enable
```

debug flexconnect aaa

FlexConnectバックアップRADIUSサーバのイベントまたはエラーのデバッグを設定するには、**debug flexconnect aaa** コマンドを使用します。

debug flexconnect aaa {**event** | **error**} {**enable** | **disable**}

構文の説明

event	FlexConnect RADIUS サーバ イベントのデバッグを設定します。
error	FlexConnect RADIUS サーバ エラーのデバッグを設定します。
enable	FlexConnect RADIUS サーバ設定のデバッグを有効にします。
disable	FlexConnect RADIUS サーバ設定のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect RADIUS サーバ イベントのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug flexconnect aaa event enable
```

debug flexconnect acl

FlexConnectアクセス コントロール リスト（ACL）のデバッグを設定するには、**debug flexconnect acl** コマンドを使用します。

debug flexconnect acl {**enable** | **disable**}

構文の説明

enable	FlexConnect ACL のデバッグを有効にします。
disable	FlexConnect ACL のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect ACL のデバッグを有効にする例を示します。

```
(Cisco Controller) >debug flexconnect acl enable
```

debug flexconnect cckm

FlexConnect Cisco Centralized Key Management（CCKM）高速ローミングのデバッグを設定するには、**debug flexconnect cckm** コマンドを使用します。

debug flexconnect cckm {**enable** | **disable**}

構文の説明

enable	FlexConnect CCKM 高速ローミング設定のデバッグを有効にします。
disable	FlexConnect CCKM 高速ローミング設定のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect CCKM 高速ローミング イベントのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug flexconnect cckm event enable
```

debug group

アクセス ポイントのグループのデバッグを設定するには、**debug group** コマンドを使用します。

debug group {**enable** | **disable**}

構文の説明

enable	アクセス ポイント グループのデバッグを有効にします。
disable	アクセス ポイント グループのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイント グループのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug group enable
```

debug fmchs

コントローラの Fixed Mobile Convergence 引き渡しサービス（FMCHS）のデバッグを設定するには、**debug fmchs** コマンドを使用します。

debug fmchs {**all** | **error** | **event** | **nmsp** | **packet**} {**enable** | **disable**}

構文の説明

all	すべての FMCHS メッセージのデバッグを設定します。
error	FMCHS エラーのデバッグを設定します。
event	FMCHS イベントのデバッグを設定します。
nmsp	FMCHS NMSP イベントのデバッグを設定します。
packet	FMCHS パケットのデバッグを設定します。
enable	FMCHS オプションのデバッグを有効にします。
disable	FMCHS オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FMCHS イベントのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug fmchs event enable
```

debug flexconnect client ap

FlexConnect クライアント アクセス ポイントの MAC アドレスをデバッグするには、**debug flexconnect client ap** コマンドを使用します。

debug flexconnect client ap *ap-name* {**add** | **delete**} *MAC-address1 MAC-address2 MAC-address3 MAC-address4*

構文の説明

add	グループに MAC アドレスを追加します。
delete	グループから MAC アドレスを削除します。
MAC-address	クライアントの MAC アドレス

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

次に、FlexConnect クライアント AP の 'room' MAC アドレスをデバッグする例を示します。

```
(Cisco Controller) >debug flexconnect client ap room add 00.0c.41.07.33.a6
0A.0c.52.17.97.b6
```

debug flexconnect client ap syslog

FlexConnect クライアント AP の syslog サーバのデバッグ ロギングを設定するには、**debug flexconnect client ap** コマンドを使用します。

debug flexconnect client ap *ap-name* **syslog** {*ip-address* | **disable**}

構文の説明

ip-address	デバッグ ロギング用に syslog サーバ IP アドレスを設定します。
disable	Syslog サーバへのデバッグ ロギングを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

次に、FlexConnect クライアント AP 'room' のデバッグ ログ用に syslog サーバを設定する例を示します。

```
(Cisco Controller) >debug flexconnect client ap room syslog 192.168.1.1
```

debug flexconnect client group

FlexConnect クライアント グループの MAC アドレスをデバッグするには、**debug flexconnect client group** コマンドを使用します。

debug flexconnect client group *group-name* {**add** | **delete**} *MAC-address1 MAC-address2 MAC-address3 MAC-address4*

構文の説明

add	グループに MAC アドレスを追加します。
delete	グループから MAC アドレスを削除します。
MAC-address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

次に、FlexConnect クライアント グループの MAC アドレスをデバッグする例を示します。

```
(Cisco Controller) >debug flexconnect client group school add 00.0c.41.07.33.a6
0A.0c.52.17.97.b6
```

debug flexconnect client group syslog

FlexConnect グループ アクセス ポイントの syslog をデバッグするには、**debug flexconnect client group** コマンドを使用します。

debug flexconnect client group *group-name* **syslog** *ip-address* | *disable*

構文の説明

ip-address	デバッグ ロギング用に syslog サーバ IP アドレスを設定します。
disable	Syslog サーバへのデバッグ ロギングを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

次に、FlexConnect クライアント グループ 'school' をデバッグ ロギング用に設定する例を示します。

```
(Cisco Controller) >debug flexconnect client group school syslog 192.168.1.1
```

debug flexconnect group

FlexConnect アクセス ポイント グループのデバッグを設定するには、**debug flexconnect group** コマンドを使用します。

debug flexconnect group {**enable** | **disable**}

構文の説明

enable	FlexConnect アクセス ポイント グループのデバッグを有効にします。
disable	FlexConnect アクセス ポイント グループのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnectアクセス ポイント グループのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug flexconnect group enable
```

debug ft

802.11r のデバッグを設定するには、**debug ft** コマンドを使用します。

debug ft {**events** | **keys**} {**enable** | **disable**}

構文の説明

events	802.11r イベントのデバッグを設定します。
keys	802.11r キーのデバッグを設定します。
enable	802.11r オプションのデバッグを有効にします。
disable	802.11r オプションのデバッグを無効にします。

コマンド デフォルト

なし

次に、802.11r のデバッグを有効にする例を示します。

```
(Cisco Controller) >debug ft events enable
```

debug hotspot

ホット スポット イベントまたはパケットのデバッグを設定するには、**debug hotspot** コマンドを使用します。

debug hotspot {**events** | **packets**} {**enable** | **disable**} {**enable** | **disable**}

構文の説明

events	ホットスポット イベントのデバッグを設定します。
packets	ホットスポット パケットのデバッグを設定します。
enable	ホットスポット オプションのデバッグを有効にします。
disable	ホットスポット オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ホットスポット イベントのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug hotspot events enable
```

debug ipv6

IPv6 オプションのデバッグを設定するには、**debug ipv6** コマンドを使用します。

debug ipv6 {**all** | **bt** | **classifier** | **errors** | **events** | **filter** | **fsm** | **gleaner** | **hwapi** | **memory** | **ndsuppress** | **parser** | **policy** | **ra_throttler** | **switcher**} {**enable** | **disable**}

構文の説明

all	すべての IPv6 情報のデバッグを設定します。
bt	IPv6 ネイバー バインディング テーブルのデバッグを設定します。
classifier	IPv6 パケット分類子のデバッグを設定します。
errors	IPv6 エラーのデバッグを設定します。
events	IPv6 イベントのデバッグを設定します。
filter	IPv6 のデバッグのためのフィルタを設定します。
fsm	IPv6 有限ステート マシン（FSM）のデバッグを設定します。
gleaner	IPv6 グリーナーのデバッグを設定します。エントリの学習は gleaning（グリーニング、収集）と呼ばれます。
hwapi	IPv6 ハードウェア API のデバッグを設定します。
memory	IPv6 バインディング テーブル メモリ使用量のデバッグを設定します。
ndsuppress	抑制された IPv6 ネイバー探索のデバッグを設定します。
parser	IPv6 パーサーのデバッグを設定します。
policy	IPv6 ポリシーのデバッグを設定します。
ra_throttler	IPv6 ルータ アドバタイジング スロットラのデバッグを設定します。
switcher	IPv6 スイッチャのデバッグを設定します。
enable	IPv6 オプションのデバッグを有効にします。
disable	IPv6 オプションのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IPv6 ポリシーのデバッグを設定する例を示します。

```
(Cisco Controller) >debug ipv6 policy enable
```

debug コマンド：j ～ q

- debug l2age （1318 ページ）
- debug mac （1319 ページ）
- debug mdns all （1320 ページ）
- debug mdns detail （1321 ページ）
- debug mdns error （1322 ページ）
- debug mdns message （1323 ページ）
- debug mdns ha （1324 ページ）
- debug memory （1325 ページ）
- debug mesh security （1326 ページ）
- debug mesh convergence （1327 ページ）
- debug mobility （1328 ページ）
- debug nac （1330 ページ）
- debug nmsp （1331 ページ）
- debug ntp （1332 ページ）
- debug packet error （1333 ページ）
- debug packet logging （1334 ページ）
- debug pem （1337 ページ）
- debug pm （1338 ページ）
- debug poe （1340 ページ）
- debug policy （1341 ページ）
- debug profiling （1342 ページ）

debug l2age

レイヤ 2 Age タイムアウト メッセージのデバッグを設定するには、**debug l2age** コマンドを使用します。

debug l2age {**enable** | **disable**}

構文の説明

enable	Layer2 Age 設定のデバッグを有効にします。
disable	Layer2 Age 設定のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Layer2 Age 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug l2age enable
```

関連コマンド

debug disable-all

debug mac

クライアント MAC アドレスのデバッグを設定するには、**debug mac** コマンドを使用します。

debug mac {**disable** | **addr** *MAC*}

構文の説明

disable	MAC アドレスを使用してクライアントのデバッグを無効にします。
addr	MAC アドレスを使用してクライアントのデバッグを設定します。
MAC	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAC アドレスを使用してクライアントのデバッグを設定する例を示します。

```
(Cisco Controller) > debug mac addr 00.0c.41.07.33.a6
```

関連コマンド

debug disable-all

debug mdns all

すべてのマルチキャスト DNS（mDNS）メッセージ、詳細、およびエラーをデバッグするには、**debug mdns all** コマンドを使用します。

debug mdns all {**enable** | **disable**}

構文の説明

enable	すべての mDNS メッセージ、詳細、エラーのデバッグを有効にします。
disable	すべての mDNS メッセージ、詳細、エラーのデバッグを無効にします。

コマンド デフォルト

デフォルトでは、すべての mDNS メッセージ、詳細、エラーのデバッグは無効です。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、すべての mDNS メッセージ、詳細、およびエラーのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug mdns all enable
```

関連コマンド

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns error

debug mdns detail

debug mdns detail

マルチキャスト DNS（mDNS）詳細をデバッグするには、**debug mdns detail** コマンドを使用します。

debug mdns detail {**enable** | **disable**}

構文の説明

enable	mDNS 詳細のデバッグを有効にします。
disable	mDNS 詳細のデバッグを無効にします。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、mDNS 詳細のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug mdns detail enable
```

関連コマンド

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns error

マルチキャスト DNS（mDNS）エラーをデバッグするには、**debug mdns error** コマンドを使用します。

debug mdns error {**enable** | **disable**}

構文の説明

enable	mDNS エラーのデバッグを有効にします。
disable	mDNS エラーのデバッグを無効にします。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、mDNS エラーのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug mdns error enable
```

関連コマンド

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns detail

debug mdns message

debug mdns message

マルチキャストDNS（mDNS）メッセージをデバッグするには、**debug mdns message** コマンドを使用します。

debug mdns message {**enable** | **disable**}

構文の説明

enable	mDNSメッセージのデバッグを有効にします。
disable	mDNSメッセージのデバッグを無効にします。

コマンド デフォルト

ディセーブル

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、mDNS メッセージのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug mdns message enable
```

関連コマンド

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns ha

すべてのマルチキャスト ドメイン ネーム システム（mDNS）高可用性（HA）メッセージをデバッグするには、**debug mdns ha** コマンドを使用します。

debug mdns ha {**enable** | **disable**}

構文の説明

enable	すべての mDNS HA メッセージのデバッグを有効にします。
disable	すべての mDNS HA メッセージのデバッグを無効にします。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**debug mdns all** コマンドが有効になると自動的に有効になります。

次に、すべての mDNS HA メッセージのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug mdns ha enable
```

debug memory

Cisco WLC のメモリ割り当て時のエラーまたはイベントのデバッグを有効または無効にするには、**debug memory** コマンドを使用します。

debug memory {**errors** | **events**} {**enable** | **disable**}

構文の説明

errors	メモリ リーク エラーのデバッグを設定します。
events	メモリ リーク イベントのデバッグを設定します。
enable	メモリ リーク イベントのデバッグを有効にします。
disable	メモリ リーク イベントのデバッグを無効にします。

コマンド デフォルト

デフォルトでは、Cisco WLC のメモリ割り当て時のエラーまたはイベントのデバッグは無効です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メモリ リーク イベントのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug memory events enable
```

関連コマンド

config memory monitor errors

show memory monitor

config memory monitor leaks

debug mesh security

メッシュ セキュリティ問題のデバッグを設定するには、**debug mesh security** コマンドを使用します。

debug mesh security {**all** | **events** | **errors**} {**enable** | **disable**}

構文の説明

all	すべてのメッシュ セキュリティ メッセージのデバッグを設定します。
events	メッシュ セキュリティ イベント メッセージのデバッグを設定します。
errors	メッシュ セキュリティ エラー メッセージのデバッグを設定します。
enable	メッシュ セキュリティ エラー メッセージのデバッグを有効にします。
disable	メッシュ セキュリティ エラー メッセージのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メッシュ セキュリティ エラー メッセージのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug mesh security errors enable
```

debug mesh convergence

メッシュ コンバージェンス問題のデバッグを設定するには、**debug mesh convergence** コマンドを使用します。

debug mesh convergence

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、メッシュ コンバージェンス エラー メッセージのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug mesh convergence
mesh convergence debugging is on
```

debug mobility

ワイヤレス モビリティのデバッグを設定するには、**debug mobility** コマンドを使用します。

debug mobility {**ap-list** | **config** | **directory** | **dtls** | **handoff** | **keep-alive** | **multicast** | **oracle** | **packet** | **peer-ip** *IP-address* | **pmk** | **pmtu-discovery** | **redha**} {**enable** | **disable**}

構文の説明

ap-list	ワイヤレスモビリティのアクセス ポイント リストのデバッグを設定します。
config	ワイヤレス モビリティ設定のデバッグを設定します。
directory	ワイヤレスモビリティ エラー メッセージのデバッグを設定します。
dtls	ワイヤレスモビリティ Datagram Transport Layer Security（DTLS）オプションのデバッグを設定します。
handoff	ワイヤレスモビリティのハンドオフ メッセージのデバッグを設定します。
keep-alive	ワイヤレス モビリティ CAPWAP データ DTLS キープアライブ パケットのデバッグを設定します。
multicast	マルチキャスト モビリティ パケットのデバッグを設定します。
oracle	ワイヤレス モビリティ Oracle オプションのデバッグを開始します。
packet	ワイヤレスモビリティ パケットのデバッグを設定します。
peer-ip	着信および発信モビリティ メッセージを表示する必要があるモビリティ ピアの IP アドレスを設定します。
IP-address	着信および発信モビリティ メッセージを表示する必要があるモビリティ ピアの IP アドレス。
pmk	ワイヤレス モビリティ ペアワイズ マスター キー（PMK）のデバッグを設定します。

pmtu-discovery	ワイヤレス モビリティ パス MTU ディスカバリのデバッグを設定します。
redha	マルチキャスト モビリティ高可用性のデバッグを設定します。
enable	ワイヤレス モビリティ機能のデバッグを有効にします。
disable	ワイヤレス モビリティ機能のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、ワイヤレス モビリティ パケットのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug mobility handoff enable
```

debug nac

ネットワーク アクセス コントロール（NAC）のデバッグを設定するには、**debug nac** コマンドを使用します。

debug nac {**events** | **packet**} {**enable** | **disable**}

構文の説明

events	NAC イベントのデバッグを設定します。
packet	NAC パケットのデバッグを設定します。
enable	NAC デバッグを有効にします。
disable	NAC デバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、NAC 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug nac events enable
```

関連コマンド

show nac statistics

show nac summary

config guest-lan nac

config wlan nac

debug nmsp

ネットワーク モビリティ サービス プロトコル（NMSP）のデバッグを設定するには、**debug nmsp** コマンドを使用します。

debug nmsp {**all** | **connection** | **detail** | **error** | **event** | **message** | **packet**}

構文の説明

all	すべての NMSP メッセージのデバッグを設定します。
connection	NMSP接続イベントのデバッグを設定します。
detail	NMSP イベントのデバッグを詳細に設定します。
error	NMSP エラー メッセージのデバッグを設定します。
event	NMSP イベントのデバッグを設定します。
message	NMSP 転送および受信メッセージのデバッグを設定します。
packet	NMSP パケット イベントのデバッグを設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、NMSP 接続イベントのデバッグを設定する例を示します。

```
(Cisco Controller) > debug nmsp connection
```

関連コマンド

clear nmsp statistics

debug disable-all

config nmsp notify-interval measurement

debug ntp

ネットワーク タイム プロトコル（NTP）のデバッグを設定するには、**debug ntp** コマンドを使用します。

debug ntp {**detail** | **low** | **packet**} {**enable** | **disable**}

構文の説明

detail	詳細な NTP メッセージのデバッグを設定します。
low	NTP メッセージのデバッグを設定します。
packet	NTP パケットのデバッグを設定します。
enable	NTP デバッグを有効にします。
disable	NTP デバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、NTP 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug ntp packet enable
```

関連コマンド

debug disable-all

debug packet error

Cisco Wireless LAN Controller（WLC） CPU に送信されたパケットのデバッグを設定するには、**debug packet error** コマンドを使用します。

debug packet error {**enable** | **disable**}

構文の説明

enable	Cisco WLC CPU に送信されたパケットのデバッグを有効にします。
disable	Cisco WLC CPU に送信されたパケットのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco WLC CPU に送信されたパケットのデバッグを有効にする方法を示します。

```
(Cisco Controller) > debug packet error enable
```

debug packet logging

Cisco Wireless LAN Controller（WLC） CPUに送信されたパケットのロギングを設定するには、**debug packet logging** コマンドを使用します。

debug packet logging {**acl** | **disable** | **enable** {**rx** | **tx** | **all**} *packet_count display_size* | **format** {**hex2pcap** | **text2pcap**}}

debug packet logging acl {**clear-all** | **driver** *rule_index action npu_encap port* | **eoip-eth** *rule_index action dst src type vlan* | **eoip-ip** *rule_index action src dst proto src_port dst_port* | **eth** *rule_index action dst src type vlan* | **ip** *rule_index action src dst proto src_port dst_port* | **lwapp-dot11***rule_index action dst src bssid type* | **lwapp-ip** *rule_index action src dst proto src_port dst_port*}

構文の説明

acl	ルールに従って表示されたパケットをフィルタリングします。
disable	すべてのパケットのロギングを無効にします。
enable	すべてのパケットのロギングを有効にします。
rx	すべての受信パケットを表示します。
tx	すべての送信パケットを表示します。
all	送信パケットと受信パケットの両方を表示します。
packet_count	記録するパケットの最大数です。有効な範囲は1～65535です。デフォルト値は25です。
display_size	パケットを印刷する際の表示バイト数です。デフォルトでは、全パケットが表示されます。
format	デバッグ出力の形式を設定します。
hex2pcap	hex2pcap形式と互換性のある出力形式を設定します。Cisco IOSによって使用される標準の形式ではhex2pcapの使用がサポートされており、HTMLフロントエンドを使用してデコードできます。
text2pcap	text2pcap形式との互換性のある出力形式を設定します。この形式では、同じコンソール ログ ファイルからパケットのシーケンスをデコードできます。。
clear-all	パケットに関連するすべての既存のルールをクリアします。

driver	着信ポートまたはネットワーク プロセッサ ユニット（NPU）カプセル化タイプに基づいてパケットをフィルタ処理します。
rule_index	ルールのインデックス値は 1 ～ 6（両端の値を含む）です。
action	ルールのアクション。有効な値は **permit**、**deny**、または **disable** です。
npu_encap	パケットのフィルタ処理方法を決める NPU カプセル化タイプです。指定可能な値には、*dhcp*、*dot11-mgmt*、*dot11-probe*、*dot1x*、*eoip-ping*、*iapp*、*ip*、*lwapp*、*multicast*、*orphan-from-sta*、*orphan-to-sta*、*rbcp*、*wired-guest*または *any* です。
port	パケットの送受信用の物理ポートです。
eoip-eth	Ethernet over IP（EoIP）ペイロードのイーサネット II ヘッダーに基づいてパケットをフィルタ処理します。
dst	宛先 MAC アドレスです。
src	送信元 MAC アドレス。
type	IP アドレスなら 0x800、Address Resolution Protocol（ARP）なら 0x806 などの 2 バイト タイプ コード。「*ip*」（0x800 の代わり）や「*arp*」（0x806 の代わり）などの一般的な文字列値も入力できます。
vlan	2 バイト VLAN 識別子。
eoip-ip	EoIP ペイロードの IP ヘッダーに基づいてパケットをフィルタ処理します。
proto	プロトコル。有効な値は、*ip*、*icmp*、*igmp*、*ggp*、*ipencap*、*st*、*tcp*、*egp*、*pup*、*udp*、*hmp*、*xns-idp*、*rdp*、*iso-tp4*、*xtp*、*ddp*、*idpr-cmtp*、*rspf*、*vmtp*、*ospf*、*ipip*、および *encap* です。

src_port	*telnet*、*23*、または *any* など、ユーザ データグラム プロトコルまたは伝送制御プロトコル（UDP または TCP）の 2 バイト送信元ポート、サポートされる文字列は、*tcpmux*、*echo*、*discard*、*systat*、*daytime*、*netstat*、*qotd*、*msp*、*chargen*、*ftp-data*、*ftp*、*fsp*、*ssh*、*telnet*、*smtp*、*time*、*rlp*、*nameserver*、*whois*、*re-mail-ck*、*domain*、*mtp*、*bootps*、*bootpc*、*tftp*、*gopher*、*rje*、*finger*、*www*、*link*、*kerberos*、*supdup*、*hostnames*、*iso-tsap*、*csnet-ns*、*3com-tsmux*、*rtelnet*、*pop-2*、*pop-3*、*sunrpc*、*auth*、*sftp*、*uucp-path*、*nntp*、*ntp*、*netbios-ns*、*netbios-dgm*、*netbios-ssn*、*imap2*、*snmp*、*snmp-trap*、*cmip-man*、*cmip-agent*、*xdmcp*、*nextstep*、*bgp*、*prospero*、*irc*、*smux*、*at-rtmp*、*at-nbp*、*at-echo*、*at-zis*、*qmtp*、*z3950*、*ipx*、*imap3*、*ulistserv*、*https*、*snpp*、*saft*、*npmp-local*、*npmp-gui*、および *hmmp-ind* です。
dst_port	*telnet*、*23*、または *any* など、UDP または TCP の 2 バイト宛先ポート。サポートされる文字列は、src_port と同じです。
eth	イーサネット II ヘッダー内の値に基づいてパケットをフィルタ処理します。
ip	IP ヘッダーの値に基づいてパケットをフィルタ処理します。
lwapp-dot11	Lightweight アクセス ポイント プロトコル（LWAPP）ペイロードの 802.11 ヘッダーに基づいてパケットをフィルタ処理します。
bssid	VLAN の Basic Service Set Identifier（基本サービス セット識別子）。
lwapp-ip	LWAPP ペイロードの IP ヘッダーに基づいてパケットをフィルタ処理します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、パケットのロギングをイネーブルにする例を示します。

```
(Cisco Controller) > debug packet logging enable
```

debug pem

アクセス ポリシー マネージャのデバッグ オプションを設定するには、**debug pem** コマンドを使用します。

debug pem {**events** | **state**} {**enable** | **disable**}

構文の説明

events	ポリシー マネージャ イベントのデバッグを設定します。
state	ポリシー マネージャのステート マシンのデバッグを設定します。
enable	アクセス ポリシー マネージャのデバッグを有効にします。
disable	アクセス ポリシー マネージャのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイント マネージャのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug pem state enable
```

debug pm

セキュリティ ポリシー マネージャ モジュールのデバッグを設定するには、**debug pm** コマンドを使用します。

debug pm {**all disable** | {**config** | **hwcrypto** | **ikemsg** | **init** | **list** | **message** | **pki** | **rng** | **rules** | **sa-export** | **sa-import** | **ssh-l2tp** | **ssh-appgw** | **ssh-engine** | **ssh-int** | **ssh-pmgr** | **ssh-ppp** | **ssh-tcp**} {**enable** | **disable**}}

構文の説明

all disable	ポリシーマネージャ モジュールのすべてのデバッグを無効にします。
config	ポリシー マネージャ設定のデバッグを設定します。
hwcrypto	ハードウェア オフロードイベントのデバッグを設定します。
ikemsg	インターネット キー交換（IKE）メッセージのデバッグを設定します。
init	ポリシー マネージャ初期化イベントのデバッグを設定します。
list	ポリシーマネージャ リスト管理のデバッグを設定します。
message	ポリシー マネージャ メッセージ キュー イベントのデバッグを設定します。
pki	公開キー インフラストラクチャ（PKI）関連イベントのデバッグを設定します。
rng	ランダム番号生成のデバッグを設定します。
rules	レイヤ 3 ポリシー イベントのデバッグを設定します。
sa-export	SAエクスポート（モビリティ）のデバッグを設定します。
sa-import	SAインポート（モビリティ）のデバッグを設定します。
ssh-l2tp	ポリシーマネージャ レイヤ2 トンネリング プロトコル（l2TP）処理のデバッグを設定します。

ssh-appgw	アプリケーション ゲートウェイのデバッグを設定します。
ssh-engine	ポリシーマネージャ エンジンのデバッグを設定します。
ssh-int	ポリシーマネージャ インターセプタのデバッグを設定します。
ssh-pmgr	ポリシーマネージャのデバッグを設定します。
ssh-ppp	ポリシーマネージャ ポイントツーポイント プロトコル（PPP）処理のデバッグを設定します。
ssh-tcp	ポリシーマネージャ TCP 処理のデバッグを設定します。
enable	デバッグをイネーブルにします。
disable	デバッグをディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、PKI 関連イベントのデバッグを設定する例を示します。

```
(Cisco Controller) > debug pm pki enable
```

関連コマンド

debug disable-all

debug poe

Power over Ethernet（PoE）のデバッグを設定するには、**debug poe** コマンドを使用します。

debug poe {**detail** | **message** | **error**} {**enable** | **disable**}

構文の説明

detail	PoE 詳細ログのデバッグを設定します。
error	PoE エラー ログのデバッグを設定します。
message	PoE メッセージのデバッグを設定します。
enable	PoE ログのデバッグを有効にします。
disable	PoE ログのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、PoE のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug poe message enable
```

関連コマンド

debug disable-all

debug policy

ポリシー設定のデバッグを設定するには、**debug policy** コマンドを使用します。

debug policy {**errors** | **events**} {**enable** | **disable**}

構文の説明

errors	ポリシー エラーのデバッグを設定します。
events	ポリシー イベントのデバッグを設定します。
enable	ポリシーイベントのデバッグを有効にします。
disable	ポリシーイベントのデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ポリシー エラーのデバッグを有効にする例を示します。

```
(Cisco Controller) >  debug policy errors enable
```

debug profiling

クライアント プロファイリングのデバッグを設定するには、**debug profiling** コマンドを使用します。

debug profiling {**enable** | **disable**}

構文の説明

enable	クライアント プロファイリング（HTTP および DHCP プロファイリング）のデバッグを有効にします。
disable	クライアント プロファイリング（HTTP および DHCP プロファイリング）のデバッグを無効にします。

コマンド デフォルト

ディセーブル

次に、クライアント プロファイリングのデバッグを有効にする例を示します。

```
(Cisco Controller) >debug profiling enable
```

debug コマンド：r ～ z

- debug rbcp （1344 ページ）
- debug rfid （1345 ページ）
- debug snmp （1346 ページ）
- debug transfer （1347 ページ）
- debug voice-diag （1348 ページ）
- debug wcp （1350 ページ）
- debug web-auth （1351 ページ）
- debug wips （1352 ページ）
- debug wps sig （1353 ページ）
- debug wps mfp （1354 ページ）

debug rbcp

Router Blade Control（RBCP）デバッグ オプションを設定するには、**debug rbcp** コマンドを使用します。

debug rbcp {**all** | **detail** | **errors** | **packet**} {**enable** | **disable**}

構文の説明

all	RBCP のデバッグを設定します。
detail	RBCP 詳細のデバッグを設定します。
errors	RBCP エラーのデバッグを設定します。
packet	RBCP パケット トレースのデバッグを設定します。
enable	RBCP デバッグを有効にします。
disable	RBCP デバッグを無効にします。

コマンド デフォルト

なし

次に、RBCP 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug rbcp packet enable
```

関連コマンド

debug disable-all

debug rfid

無線周波数 ID（RFID）デバッグ オプションを設定するには、**debug rfid** コマンドを使用します。

debug rfid {**all** | **detail** | **errors** | **nmsp** | **receive**} {**enable** | **disable**}

構文の説明

all	すべての RFID のデバッグを設定します。
detail	RFID 詳細のデバッグを設定します。
errors	RFIDエラー メッセージのデバッグを設定します。
nmsp	RFID の Network Mobility Services Protocol（NMSP）メッセージのデバッグを設定します。
receive	受信した RFID タグ メッセージのデバッグを設定します。
enable	RFID デバッグを有効にします。
disable	RFID デバッグを無効にします。

コマンド デフォルト

なし

次に、RFID エラー メッセージのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug rfid errors enable
```

関連コマンド

debug disable-all

debug snmp

SNMP デバッグ オプションを設定するには、**debug snmp** コマンドを使用します。

debug snmp {**agent** | **all** | **mib** | **trap**} {**enable** | **disable**}

構文の説明

agent	SNMPエージェントのデバッグを設定します。
all	すべての SNMP メッセージのデバッグを設定します。
mib	SNMP MIB のデバッグを設定します。
trap	SNMP トラップのデバッグを設定します。
enable	SNMP デバッグを有効にします。
disable	SNMP デバッグを無効にします。

コマンド デフォルト

なし

次に、SNMP のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug snmp trap enable
```

関連コマンド

debug disable-all

debug transfer

転送デバッグ オプションを設定するには、**debug transfer** コマンドを使用します。

debug transfer {**all** | **tftp** | **trace**} {**enable** | **disable**}

構文の説明

all	すべての転送メッセージのデバッグを設定します。
tftp	TFTP 転送のデバッグを設定します。
trace	転送メッセージのデバッグを設定します。
enable	転送メッセージのデバッグを有効にします。
disable	転送メッセージのデバッグを無効にします。

コマンド デフォルト

なし

次に、転送メッセージのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug transfer trace enable
```

関連コマンド

debug disable-all

debug voice-diag

コールまたはパケット フローを追跡するには、**debug voice-diag** コマンドを使用します。

debug voice-diag {**enable** *client_mac1* ［*client_mac2*］［**verbose**］ | **disable**}

構文の説明

enable	コールに関連する音声クライアントの音声診断のデバッグを有効にします。
client_mac1	音声クライアントの MAC アドレス。
client_mac2	（任意）他の音声クライアントの MAC アドレス。 （注） 2 つの音声クライアントを最大化するために、音声診断を一度にイネーブルまたはディセーブルにできます。
verbose	（任意）コンソールに表示されるデバッグ情報をイネーブルにします。 （注） 音声診断が NCS または Prime Infrastructure から有効に設定された場合、冗長オプションは使用できません。
disable	コールに関連する音声クライアントの音声診断のデバッグを無効にします。

コマンド デフォルト

なし

使用上のガイドライン

debug voice-diag コマンドを使用するときは、次のガイドラインに従ってください。

- このコマンドを入力すると、クライアントの有効性は検査されません。
- コマンドの出力メッセージのいくつかが、NCS または Prime Infrastructure に送信されます。
- コマンドは 60 分後に自動的に期限切れになります。
- コマンドは、アクティブ コールに関連するクライアント MAC ペア間のコール フローの詳細を示します。

（注） 2 つの音声クライアントを最大化するために、音声診断を一度にイネーブルにできます。

次に、転送/アップグレード設定を有効にする例を示します。

```
(Cisco Controller) > debug voice-diag enable 00:1a:a1:92:b9:5c 00:1a:a1:92:b5:9c verbose
```

関連コマンド

show client voice-diag

show client calls

debug wcp

WLAN Control Protocol（WCP）のデバッグを設定するには、**debug wcp** コマンドを使用します。

debug wcp {**events** | **packet**} {**enable** | **disable**}

構文の説明

events	WCP イベントのデバッグを設定します。
packet	WCP パケットのデバッグを設定します。
enable	WCP 設定のデバッグを有効にします。
disable	WCP 設定のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WCP 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) >debug wcp packet enable
```

debug web-auth

Web 認証済みクライアントのデバッグを設定するには、**debug web-auth** コマンドを使用します。

debug web-auth {**redirect**{ **enable mac** *mac_address* | **disable**} | **webportal-server** {**enable** | **disable**}}

構文の説明

redirect	Web 認証され、リダイレクトされたクライアントのデバッグを設定します。
enable	Web 認証済みクライアントのデバッグを有効にします。
mac	Web 認証済みクライアントの MAC アドレスを設定します。
mac_address	Web 認証済みクライアントの MAC アドレス。
disable	Web 認証済みクライアントのデバッグを無効にします。
webportal-server	クライアントのポータル認証のデバッグを設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Web 認証され、リダイレクトされたクライアントのデバッグを有効にする例を示します。

```
(Cisco Controller) > debug web-auth redirect enable mac xx:xx:xx:xx:xx:xx
```

debug wips

ワイヤレス侵入防御システム（WIPS）のデバッグを設定するには、**debug wips** コマンドを使用します。

debug wips {**all** | **error** | **event** | **nmsp** | **packet**} {**enable** | **disable**}

構文の説明

all	すべての WIPS メッセージのデバッグを設定します。
error	WIPS エラーのデバッグを設定します。
event	WIPS イベントのデバッグを設定します。
nmsp	WIPS の Network Mobility Services Protocol（NMSP）イベントのデバッグを設定します。
packet	WIPS パケットのデバッグを設定します。
enable	WIPS のデバッグを有効にします。
disable	WIPS のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての WIPS メッセージのデバッグを有効にする方法を示します。

```
(Cisco Controller) > debug wips all enable
```

関連コマンド

debug client

debug dot11 rogue

show wps summary

show wps wips

debug wps sig

ワイヤレスプロビジョニングサービス（WPS）のシグニチャ設定のデバッグを設定するには、**debug wps sig** コマンドを使用します。

debug wps sig {**enable** | **disable**}

構文の説明

enable	WPS 設定のデバッグを有効にします。
disable	WPS 設定のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WPS シグニチャ設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug wps sig enable
```

関連コマンド

debug wps mfp

debug disable-all

debug wps mfp

WPS 管理フレーム保護（MFP）設定のデバッグを設定するには、**debug wps mfp** コマンドを使用します。

debug wps mfp {**client** | **capwap** | **detail** | **report** | **mm**} {**enable** | **disable**}

構文の説明

client	クライアント MFP メッセージのデバッグを設定します。
capwap	コントローラとアクセス ポイント間の MFP メッセージのデバッグを設定します。
detail	MFP メッセージの詳細デバッグを設定します。
report	MFP レポートのデバッグを設定します。
mm	MFP モビリティ（Cisco WLC 間）メッセージのデバッグを設定します。
enable	WPS MFP 設定のデバッグを有効にします。
disable	WPS MFP 設定のデバッグを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WPS MFP 設定のデバッグを有効にする例を示します。

```
(Cisco Controller) > debug wps mfp detail enable
```

関連コマンド

debug disable-all

debug wps sig

第 V 部

IMM コマンド

• IMM コマンド （1357 ページ）

IMM コマンド

- imm address （1358 ページ）
- imm dhcp （1359 ページ）
- imm mode （1360 ページ）
- imm restart （1361 ページ）
- imm summary （1362 ページ）
- imm username （1363 ページ）

imm address

IMM の静的 IP アドレスを設定するには、**imm address** コマンドを使用します。

imm address *ip-addr netmask gateway*

構文の説明

ip-addr	IMM の IP アドレス。
netmask	IMM のネットマスク
gateway	IMM のゲートウェイ

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

次に、IMM の静的 IP アドレスを設定する例を示します。

```
(Cisco Controller) >imm address 209.165.200.225 255.255.255.224 10.1.1.1
```

imm dhcp

IMM の DHCP を設定するには、**imm dhcp** コマンドを使用します。

imm dhcp {**enable** | **disable** | **fallback**}

構文の説明

enable	IMM の DHCP を有効にします
disable	IMM の DHCP を無効にします
fallback	IMM の DHCP を有効にします。これが失敗した場合、IMM の固定 IP を使用します。

コマンド デフォルト

IMM の DHCP は有効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IMM の DHCP を有効にする例を示します。

```
(Cisco Controller) >imm dhcp enable
```

imm mode

IMM モードを設定するには、**imm mode** コマンドを使用します。

imm mode {**shared** | **dedicated**}

構文の説明

shared	IMM を共有モードで設定します。
dedicated	IMM を専用モードで設定します。

コマンド デフォルト

dedicated

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IMM を共有モードで設定する例を示します。

```
(Cisco Controller) >imm mode
```

imm restart

IMM を再起動するには、**imm restart** コマンドを使用します。

imm restart

構文の説明		
	restart	設定を保存し、IMM を再起動します

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

imm summary

IMM パラメータを表示するには、**imm summary** コマンドを使用します。

imm summary

構文の説明

summary	IMM パラメータをリストします

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IMM の一般的な要約の例を示します。

```
(Cisco Controller) >imm summary
User ID.....................................username1
Mode..................................... Shared
DHCP..................................... Enabled
IP Address..............................  209.165.200.225
Subnet Mask.............................  255.255.255.224
Gateway.................................  10.1.1.1
```

imm username

IMM ユーザのログオン クレデンシャルを設定するには、**imm username** コマンドを使用します。

imm username *username password*

構文の説明

username	ユーザのユーザ名
password	ユーザのパスワード

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IMM ユーザのログオン クレデンシャルを設定する例を示します。

```
(Cisco Controller) >imm username username1 password1
```

第 VI 部

license コマンド

• license コマンド （1367 ページ）

license コマンド

- license activate ap-count eval （1368 ページ）
- license activate feature （1369 ページ）
- license add ap-count （1370 ページ）
- license add feature （1371 ページ）
- license clear （1372 ページ）
- license comment （1373 ページ）
- license deactivate ap-count eval （1374 ページ）
- license deactivate feature （1375 ページ）
- license delete ap-count （1376 ページ）
- license delete feature （1377 ページ）
- license install （1378 ページ）
- license modify priority （1379 ページ）
- license revoke （1381 ページ）
- license save （1382 ページ）
- license smart （1383 ページ）

license activate ap-count eval

Cisco Flex 7500 シリーズおよび Cisco 8500 シリーズ ワイヤレス LAN コントローラのアクセスポイント評価ライセンスをアクティブ化するには、 **license activate ap-count eval** コマンドを使用します。

license activate ap-count eval

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトで、リリース 7.3 Cisco Flex 7500 シリーズ コントローラと Cisco 8500 シリーズ ワイヤレス LAN コントローラは 6000 AP をサポートします。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このライセンスをアクティブ化すると、コントローラによって、所定のライセンスのエンドユーザ ライセンス契約（EULA）の受け入れまたは拒否を求めるプロンプトが表示されます。コントローラに接続された現在の AP 数よりも少ない APS 数をサポートするライセンスをアクティブ化した場合、アクティベーション コマンドは失敗します。

次に、Cisco Flex 7500 シリーズ コントローラで評価版 AP-count ライセンスをアクティブ化する例を示します。

```
(Cisco Controller) > license activate ap-count eval
```

license activate feature

Cisco Flex 7500 シリーズおよび Cisco 8500 シリーズ ワイヤレス LAN コントローラで機能ライセンスをアクティブ化するには、 **license activate feature** コマンドを使用します。

license activate feature *license_name*

構文の説明

license_name	機能ライセンスの名前。ライセンス名は最大 50 文字の文字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Flex 7500 シリーズ コントローラで Data DTLS 機能のライセンスをアクティブ化する例を示します。

```
(Cisco Controller) > license activate feature data-DTLS
```

license add ap-count

AP ライセンスが Cisco Flex 7500 および 8500 シリーズ ワイヤレス LAN コントローラでサポートできるアクセス ポイント（AP）数を設定するには、**license add ap-count** コマンドを使用します。

license add ap-count *count*

構文の説明

count	AP ライセンスでサポートする AP の数。範囲は 1 からコントローラがサポートできる AP の最大数までです。数は 5 の倍数である必要があります。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Right to Use（RTU）ライセンスがあると、エンドユーザ ライセンス契約（EULA）を受け入れた後、希望する AP ライセンス数をコントローラ上でイネーブルにできます。これで、外部ツールを使用せずに、簡単にコントローラに AP 数を追加できます。RTU ライセンスは、Cisco Flex 7500 および 8500 シリーズ ワイヤレス LAN コントローラのみで使用できます。

このコマンドを使用して、既存の AP ライセンス数を増やすことができます。コントローラに接続された現在の AP 数よりも少ない APS 数をサポートするライセンスをアクティブ化した場合、アクティベーション コマンドは失敗します。

次に、Cisco Flex 7500 シリーズ コントローラに AP ライセンス数を設定する例を示します。

```
(Cisco Controller) > license add ap-count 5000
```

license add feature

Cisco 5520 WLC、Cisco Flex 7510 WLC、Cisco 8510 WLC、Cisco 8540 WLC、および Cisco 仮想コントローラの機能にライセンスを追加するには、 **license add feature** コマンドを使用します。

license add feature *license_name*

構文の説明

license_name	機能ライセンスの名前。ライセンス名は最大 50 文字の文字で、大文字と小文字を区別します。data_encryption などがあります。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。 このコマンドは、Cisco Flex 7510 WLC と Cisco 8510 WLC に適用されます。
8.1	このコマンドは、Cisco 5520 WLC、Cisco Flex 7510 WLC、Cisco 8510 WLC、Cisco 8540 WLC、および Cisco vWLC に適用されます。

次に、data_encryption 機能ライセンスを追加する例を示します。

```
(Cisco Controller) > license add feature data_encryption
```

license clear

Cisco 5500 シリーズ コントローラからライセンスを削除するには、**license clear** コマンドを使用します。

license clear *license_name*

構文の説明

license_name	ライセンスの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

有効期限の切れた評価ライセンスや、未使用のライセンスを削除できます。有効期限前のライセンス、永久ベース イメージ ライセンス、またはコントローラによって使用されるライセンスは削除できません。

次に、wplus-ap-count という名前のライセンスの設定を削除する例を示します。

```
(Cisco Controller) > license clear wplus-ap-count
```

license comment

Cisco 5500 シリーズ コントローラでライセンスにコメントを追加したり、ライセンスからコメントを削除したりするには、**license comment** コマンドを使用します。

license comment {**add** | **delete**} *license_name comment_string*

構文の説明

add	コメントを追加します。
delete	コメントを削除します。
license_name	ライセンスの名前。
comment_string	ライセンスのコメント。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ライセンス名 wplus-ap-count にコメント「wplus ap count license」を追加する例を示します。

```
(Cisco Controller) > license comment add wplus-ap-count Comment for wplus ap count license
```

license deactivate ap-count eval

Cisco Flex 7500 シリーズおよび Cisco 8500 シリーズ ワイヤレス LAN コントローラのアクセスポイント評価ライセンスを非アクティブにするには、 **license deactivate ap-count eval** コマンドを使用します。

license deactivate ap-count eval

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Flex 7500 シリーズ コントローラで AP 評価ライセンスを非アクティブにする例を示します。

```
(Cisco Controller) > license deactivate ap-count eval
```

license deactivate feature

Cisco Flex 7500 シリーズおよび Cisco 8500 シリーズ ワイヤレス LAN コントローラで機能ライセンスを非アクティブにするには、 **license deactivate feature** コマンドを使用します。

license deactivate feature *license_name*

構文の説明

license_name	機能ライセンスの名前。ライセンス名は最大 50 文字の文字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Flex 7500 シリーズ コントローラで Data DTLS 機能のライセンスを非アクティブにする例を示します。

```
(Cisco Controller) > license deactivate feature data_DTLS
```

license delete ap-count

Cisco Flex 7500 シリーズおよび Cisco 8500 シリーズ ワイヤレス LAN コントローラのアクセスポイント（AP）数ライセンスを削除するには、 **license delete ap-count** コマンドを使用します。

license delete ap-count *count*

構文の説明

count	AP ライセンスでサポートする AP の数。範囲は 1 からコントローラがサポートできる AP の最大数までです。数は 5 の倍数である必要があります。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Flex 7500 シリーズ コントローラの AP 数ライセンスを削除する例を示します。

```
(Cisco Controller) > license delete ap-count 5000
```

license delete feature

Cisco Flex 7500 シリーズおよび Cisco 8500 シリーズ ワイヤレス LAN コントローラの機能のライセンスを削除するには、 **license delete feature** コマンドを使用します。

license delete feature *license_name*

構文の説明

license_name	機能ライセンスの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco Flex 7500 シリーズ コントローラの高可用性機能のライセンスを削除する例を示します。

```
(Cisco Controller) > license delete feature high_availability
```

license install

Cisco 5500 シリーズ コントローラにライセンスをインストールするには、**license install** コマンドを使用します。

license install *url*

構文の説明

url	TFTP サーバの URL（tftp://server_ip/path/filename）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラにインストールする base-ap-count ライセンスと wplus-ap-count ライセンスのアクセス ポイント数は、同一にすることをお勧めします。コントローラの base-ap-count ライセンスが 100 である場合に、wplus-ap-count ライセンス 12 をインストールすると、そのコントローラではベース ライセンスの使用時に最大 100 個のアクセス ポイントをサポートしますが、WPLUS ライセンスの使用時には最大 12 個のアクセス ポイントしかサポートされません。

インストールする WPLUS ライセンスのアクセス ポイント数をコントローラのベース ライセンスより多くすることはできません。たとえば、既存の base-ap-count ライセンスが 12 のコントローラに wplus-ap-count ライセンス 100 を適用することはできません。このようなライセンスを登録しようとすると、ライセンス登録が失敗したことを示すエラー メッセージが表示されます。wplus-ap-count 100 ライセンスをアップグレードする前に、コントローラの base-ap-count ライセンスを 100 または 250 にアップグレードする必要があります。

次に、URL tftp://10.10.10.10/path/license.lic からライセンスをコントローラにインストールする例を示します。

```
(Cisco Controller) > license install tftp://10.10.10.10/path/license.lic
```

license modify priority

Cisco 5500 シリーズ コントローラで base-ap-count または wplus-ap-count 評価ライセンスの優先順位を上げる、または下げるには、**license modify priority** コマンドを使用します。

license modify priority *license_name* {**high** | **low**}

構文の説明

license_name	ap-count 評価ライセンス。
high	ap-count評価ライセンスの優先順位を変更します。
low	ap-count評価ライセンスの優先順位を変更します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

アクセス ポイント数の多いライセンスにアップグレードする場合は、永久バージョンのライセンスにアップグレードする前に評価ライセンスを試すことができます。たとえば、現在、アクセス ポイント数が 50 の永久ライセンスを使用しており、アクセス ポイント数が 100 の評価ライセンスを試す場合、60 日間評価ライセンスを試すことができます。

ap-count 評価ライセンスの優先順位は、デフォルトで low に設定されるので、コントローラではap-count永久ライセンスが使用されます。アクセス ポイント数を増やした評価ライセンスを試す場合は、優先順位を high に変更する必要があります。そのような高容量は必要ないと判断した場合は、ap-count 評価ライセンスの優先順位を下げて、コントローラで永久ライセンスが使用されるようにすることができます。

（注） 優先順位を設定できるのは、ap-count 評価ライセンスに限られます。ap-count 永久ライセンスの優先順位は常に medium であり、設定できません。

（注） ap-count 評価ライセンスが WPLUS ライセンスであり、ap-count 永久ライセンスがベース ライセンスである場合は、フィーチャ セットも WPLUS に変更する必要があります。

（注） 操作の中断を避けるために、コントローラは、評価ライセンスの有効期限が切れてもライセンスを切り替えません。永久ライセンスに戻すには、コントローラをリブートする必要があります。リブート後に、期限切れになった評価ライセンスと同じフィーチャ セット レベルにコントローラがデフォルト設定されます。同じフィーチャ セット レベルの永久ライセンスがインストールされていない場合、コントローラは、別のレベルの永久ライセンスまたは有効期限の切れていない評価ライセンスを使用します。

次に、wplus-ap-count の優先度を high に設定する例を示します。

```
(Cisco Controller) > license modify priority wplus-ap-count high
```

license revoke

Cisco 5500 シリーズ WLC でライセンスを再ホストするには、**license revoke** コマンドを使用します。

license revoke {*permission_ticket_url* | **rehost** *rehost_ticket_url*}

構文の説明

permission_ticket_url	権限チケットを保存した TFTP サーバの URL（tftp://server_ip/path/filename）。
rehost	再ホスト ライセンスの設定を指定します。
rehost_ticket_url	再ホスト チケットを保存した TFTP サーバの URL（tftp://server_ip/path/filename）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ライセンスを取り消す前に、**license save credential** *url* コマンドを使用してデバイスのクレデンシャルを保存します。

永久ベース イメージ ライセンスを除く、すべての永久ライセンスを再ホストできます。評価ライセンスおよび永久ベース イメージ ライセンスは再ホストできません。

ライセンスを再ホストするには、コントローラから認証情報を生成し、その情報を使用して、Cisco ライセンス サイト（https://tools.cisco.com/SWIFT/LicensingUI/Quickstart）からライセンスを無効にするための権限チケットを取得する必要があります。次に、再ホスト チケットを取得し、そのチケットを使用して、ライセンスをインストールするコントローラ用のライセンス インストール ファイルを取得します。

ライセンスの再ホストの詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』第 4 章「Installing and Configuring Licenses」を参照してください。

次に、保存された権限チケット URL tftp://10.10.10.10/path/permit_ticket.lic からライセンス設定を取り消す例を示します。

```
(Cisco Controller) > license revoke tftp://10.10.10.10/path/permit_ticket.lic
```

次に、保存された再ホスト チケット URL tftp://10.10.10.10/path/rehost_ticket.lic からライセンス設定を取り消す例を示します。

```
(Cisco Controller) > license revoke rehost tftp://10.10.10.10/path/rehost_ticket.lic
```

license save

Cisco 5500 シリーズ コントローラにインストールしたすべてのライセンスのバックアップ コピーを保存するには、**license save** コマンドを使用します。

license save *credential url*

構文の説明

credential	デバイス クレデンシャル情報。
url	TFTP サーバの URL（tftp://server_ip/path/filename）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

license revoke コマンドを使用してライセンスを取り消す前に、デバイス クレデンシャルを保存します。

次に、tftp://10.10.10.10/path/cred.lic でインストールされたすべてのライセンスまたはライセンス クレデンシャルのバックアップ コピーを保存する例を示します。

```
(Cisco Controller) > license save credential tftp://10.10.10.10/path/cred.lic
```

license smart

シスコ スマート ソフトウェア ライセンシング プラットフォームを使用してデバイスを登録または登録解除するには、**license smart** コマンドを使用します。

license smart {**register** | **deregister**} *idtoken*

構文の説明

register	シスコ スマート ソフトウェア ライセンス プラットフォームにデバイスを追加し、有効化します。
deregister	シスコ スマート ソフトウェア ライセンス プラットフォームのデバイスを削除します。
idtoken	デバイスの固有の ID。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、シスコ スマート ソフトウェア ライセンス プラットフォームにデバイスを登録する方法を示します。

```
(Cisco Controller) > license smart register
RkMxJbjKMV11hmpgh46mAgXSNKmticyJzu0xDfYgf8xflkiYbZsCqprt
```

第 VII 部

show コマンド

- show コマンド：802.11 （1387 ページ）
- show コマンド：a ～ i （1403 ページ）
- show コマンド：j ～ q （1611 ページ）
- show コマンド：r ～ z （1731 ページ）

show コマンド：802.11

- show 802.11 （1388 ページ）
- show 802.11 （1390 ページ）
- show 802.11 cleanair （1392 ページ）
- show 802.11 cleanair air-quality summary （1394 ページ）
- show 802.11 cleanair air-quality worst （1395 ページ）
- show 802.11 cleanair device ap （1396 ページ）
- show 802.11 cleanair device type （1397 ページ）
- show 802.11 cu-metrics （1399 ページ）
- show 802.11 extended （1400 ページ）
- show 802.11 media-stream （1402 ページ）

show 802.11

802.11a、802.11b/g、または 802.11h の基本的なネットワーク設定を表示するには、**show 802.11** コマンドを使用します。

show 802.11 {**a** | **b** | **h**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
h	802.11h ネットワークを指定します。

コマンド デフォルト

なし。

次に、802.11a の基本的なネットワーク設定を表示する例を示します。

```
> show 802.11a
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 Rate................................. Mandatory
    802.11a 9M Rate................................. Supported
    802.11a 12M Rate................................ Mandatory
    802.11a 18M Rate................................ Supported
    802.11a 24M Rate................................ Mandatory
    802.11a 36M Rate................................ Supported
    802.11a 48M Rate................................ Supported
    802.11a 54M Rate................................ 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
802.11n Status:
    A-MPDU Tx:
        Priority 0.................................. Enabled
        Priority 1.................................. Disabled
        Priority 2.................................. Disabled
        Priority 3.................................. Disabled
        Priority 4.................................. Disabled
```

```
        Priority 5.............................. Disabled
        Priority 6.............................. Disabled
        Priority 7.............................. Disabled
Beacon Interval................................. 100
CF Pollable mandatory........................... Disabled
CF Poll Request mandatory....................... Disabled
--More-- or (q)uit
CFP Period...................................... 4
CFP Maximum Duration............................ 60
Default Channel................................. 36
Default Tx Power Level.......................... 0
DTPC Status..................................... Enabled
Fragmentation Threshold......................... 2346
TI Threshold.................................... -50
Legacy Tx Beamforming setting................... Disabled
Traffic Stream Metrics Status................... Enabled
Expedited BW Request Status..................... Disabled
World Mode...................................... Enabled
EDCA profile type............................... default-wmm
Voice MAC optimization status................... Disabled
Call Admission Control (CAC) configuration
Voice AC:
   Voice AC - Admission control (ACM)............ Disabled
   Voice max RF bandwidth........................ 75
   Voice reserved roaming bandwidth.............. 6
   Voice load-based CAC mode..................... Disabled
   Voice tspec inactivity timeout................ Disabled
   Voice Stream-Size............................. 84000
   Voice Max-Streams............................. 2
Video AC:
   Video AC - Admission control (ACM)............ Disabled
   Video max RF bandwidth........................ Infinite
   Video reserved roaming bandwidth.............. 0
```

次に、802.11h の基本的なネットワーク設定を表示する例を示します。

```
> show 802.11h
802.11h ..................................... powerconstraint : 0
802.11h ..................................... channelswitch : Disable
802.11h ..................................... channelswitch mode : 0
```

関連コマンド

show ap stats

show ap summary

show client summary

show network

show network summary

show port

show wlan

show 802.11

802.11a、802.11b/g、または 802.11h の基本的なネットワーク設定を表示するには、**show 802.11** コマンドを使用します。

show 802.11 {**a** | **b** | **h**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
h	802.11h ネットワークを指定します。

コマンド デフォルト

なし。

次に、802.11a の基本的なネットワーク設定を表示する例を示します。

```
> show 802.11a
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 Rate................................. Mandatory
    802.11a 9M Rate................................. Supported
    802.11a 12M Rate................................ Mandatory
    802.11a 18M Rate................................ Supported
    802.11a 24M Rate................................ Mandatory
    802.11a 36M Rate................................ Supported
    802.11a 48M Rate................................ Supported
    802.11a 54M Rate................................ 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
802.11n Status:
    A-MPDU Tx:
        Priority 0.................................. Enabled
        Priority 1.................................. Disabled
        Priority 2.................................. Disabled
        Priority 3.................................. Disabled
        Priority 4.................................. Disabled
```

```
        Priority 5.............................. Disabled
        Priority 6.............................. Disabled
        Priority 7.............................. Disabled
Beacon Interval................................. 100
CF Pollable mandatory........................... Disabled
CF Poll Request mandatory....................... Disabled
--More-- or (q)uit
CFP Period...................................... 4
CFP Maximum Duration............................ 60
Default Channel................................. 36
Default Tx Power Level.......................... 0
DTPC Status..................................... Enabled
Fragmentation Threshold......................... 2346
TI Threshold.................................... -50
Legacy Tx Beamforming setting................... Disabled
Traffic Stream Metrics Status................... Enabled
Expedited BW Request Status..................... Disabled
World Mode...................................... Enabled
EDCA profile type............................... default-wmm
Voice MAC optimization status................... Disabled
Call Admission Control (CAC) configuration
Voice AC:
   Voice AC - Admission control (ACM)............ Disabled
   Voice max RF bandwidth........................ 75
   Voice reserved roaming bandwidth.............. 6
   Voice load-based CAC mode..................... Disabled
   Voice tspec inactivity timeout................ Disabled
   Voice Stream-Size............................. 84000
   Voice Max-Streams............................. 2
Video AC:
   Video AC - Admission control (ACM)............ Disabled
   Video max RF bandwidth........................ Infinite
   Video reserved roaming bandwidth.............. 0
```

次に、802.11h の基本的なネットワーク設定を表示する例を示します。

```
> show 802.11h
802.11h ..................................... powerconstraint : 0
802.11h ..................................... channelswitch : Disable
802.11h ..................................... channelswitch mode : 0
```

関連コマンド

show ap stats

show ap summary

show client summary

show network

show network summary

show port

show wlan

show 802.11 cleanair

マルチキャスト ダイレクト設定の状態を表示するには、**show 802.11 cleanair** コマンドを使用します。

show 802.11{**a** | **b** | **h**} **cleanair config**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
h	802.11h ネットワークを指定します。
config	ネットワークの cleanair の設定を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a cleanair の設定を表示する例を示します。

```
(Cisco Controller) > show 802.11a cleanair
Clean Air Solution..............................  Enabled
Air Quality Settings:
    Air Quality Reporting.......................  Enabled
    Air Quality Reporting Period (min)..........  15
    Air Quality Alarms..........................  Enabled
   Air Quality Alarm Threshold.................. 35 Interference Device
 Settings:
    Interference Device Reporting...............  Enabled
    Interference Device Types:
        TDD Transmitter.........................  Disabled
        Jammer..................................  Disabled
        Continuous Transmitter..................  Disabled
        DECT-like Phone.........................  Disabled
        Video Camera............................  Disabled
        WiFi Inverted...........................  Disabled
        WiFi Invalid Channel....................  Disabled
        SuperAG.................................  Disabled
        Radar...................................  Disabled
        Canopy..................................  Disabled
        WiMax Mobile............................  Disabled
        WiMax Fixed.............................  Disabled
Interference Device Alarms...................  Enabled
    Interference Device Types Triggering Alarms:
```

```
        TDD Transmitter..................... Disabled
        Jammer.............................. Disabled
        Continuous Transmitter.............. Disabled
        DECT-like Phone..................... Disabled
        Video Camera........................ Disabled
        WiFi Inverted....................... Disabled
        WiFi Invalid Channel................ Disabled
        SuperAG............................. Disabled
        Radar............................... Disabled
        Canopy.............................. Disabled
        WiMax Mobile........................ Disabled
        WiMax Fixed......................... Disabled Additional
Clean Air Settings:
    CleanAir Event-driven RRM State..... Enabled
    CleanAir Driven RRM Sensitivity..... Medium
    CleanAir Persistent Devices state..... Disabled
```

show 802.11 cleanair air-quality summary

802.11 ネットワークの電波品質のサマリー情報を表示するには、**show 802.11 cleanair air-quality summary** コマンドを使用します。

show 802.11 {**a** | **b** | **h**} **cleanair air-quality summary**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
h	802.11h ネットワークを指定します。
summary	802.11 無線帯域電波品質情報のサマリーを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークの電波品質のサマリー情報を表示する例を示します。

```
(Cisco Controller) > show 802.11a cleanair air-quality summary
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name            Channel  Avg AQ  Min AQ  Interferers  DFS
------------------ -------  ------  ------  -----------  ---
CISCO_AP3500       36   95  70   0
CISCO_AP3500     40   93  75   0
```

show 802.11 cleanair air-quality worst

802.11 ネットワークの最も深刻な電波品質の情報を表示するには、**show 802.11 cleanair air-quality worst** コマンドを使用します。

show 802.11{**a** | **b** | **h**} **cleanair air-quality worst**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
h	802.11h ネットワークを指定します。
worst	802.11 ネットワークの最も深刻な電波品質の情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークの最も深刻な電波品質の情報を表示する例を示します。

```
(Cisco Controller) > show 802.11 cleanair air-quality worst
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name            Channel  Avg AQ  Min AQ  Interferers  DFS
------------------ -------  ------  ------  -----------  ---
CISCO_AP3500       1   83  57   3   5
```

show 802.11 cleanair device ap

802.11 無線帯域のデバイス アクセス ポイントの情報を表示するには、**show 802.11 cleanair device ap** コマンドを使用します。

show 802.11 {**a** | **b** | **h**} **cleanair device ap** *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
h	802.11h ネットワークを指定します。
cisco_ap	特定のアクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a ネットワークのデバイス アクセス ポイントを表示する例を示します。

```
(Cisco Controller) > show 802.11a cleanair device ap AP_3500
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   c2:f7:40:00:00:03  0x8001 DECT phone  CISCO_AP3500  1    -43     3
      149,153,157,161
2   c2:f7:40:00:00:51  0x8002 Radar       CISCO_AP3500  1    -81     2
    153,157,161,165
3   c2:f7:40:00:00:03  0x8005 Canopy      CISCO_AP3500  2    -62     2
     153,157,161,165
```

show 802.11 cleanair device type

802.11 無線帯域の特定のアクセス ポイントによって検出されたすべての干渉デバイス タイプの情報を表示するには、**show 802.11 cleanair device type** コマンドを使用します。

show 802.11{**a** | **b** | **h**} **cleanair device type** *device_type*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
h	802.11h ネットワークを指定します。
device_type	指定した無線帯域の干渉デバイスのタイプ。デバイス タイプは次のいずれかです。 • tdd-tx：Tdd トランスミッタのデバイス情報。 • jammer：電波妨害デバイス情報。 • cont-tx：連続トランスミッタのデバイス情報。 • dect-like：Dect-like 電話デバイス情報。 • video：ビデオ デバイス情報。 • 802.11-inv：WiFi 反転デバイス情報。 • 802.11-nonstd：非標準 WiFi デバイス情報。 • superag：Superag デバイス情報。 • canopy：Canopy デバイス情報。 • wimax-mobile：WiMax モバイル デバイス情報。 • wimax-fixed：WiMax 固定デバイス情報。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークに指定されたアクセス ポイントによって検出されたすべての干渉源情報を表示する例を示します。

```
(Cisco Controller) > show 802.11a cleanair device type canopy
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
--- ------------------ ------ ---------- --------------- ---- -----
---- -------------
1c2:f7:40:00:00:03  0x8005 Canopy          CISCO_AP3500  2    -62
 2     153,157,161,165
```

show 802.11 cu-metrics

アクセス ポイントのチャネル使用率メトリックを表示するには、**show 802.11 cu-metrics** コマンドを使用します。

show 802.11{**a** | **b**} **cu-metrics** *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
cisco_ap	アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show 802.11a cu-metrics** コマンドの出力例を示します。

```
(Cisco Controller) > show 802.11a cu-metrics AP1
AP Interface Mac:           30:37:a6:c8:8a:50
Measurement Duration:       90sec
 Timestamp               Thu Jan 27 09:08:48 2011
   Channel Utilization stats
   =================
     Picc (50th Percentile)..................... 0
     Pib (50th Percentile)...................... 76
     Picc (90th Percentile)..................... 0
     Pib (90th Percentile)...................... 77
 Timestamp               Thu Jan 27 09:34:34 2011
```

show 802.11 extended

アクセス ポイント無線の拡張設定を表示するには、**show 802.11 extended** コマンドを使用します。

show 802.11 {**a** | **b**} **extended**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
extended	802.11a/b 無線の拡張設定を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	コマンド出力は、Rx SOP しきい値を含むように拡張されました。

次に、無線の拡張設定を表示する例を示します。

```
(Cisco Controller) > show 802.11a extended
Default 802.11a band radio extended configurations:
    beacon period 300, range 60;
    multicast buffer 45, rate 200;
    RX SOP -80; CCA threshold -90;
AP0022.9090.b618 00:24:97:88:99:60
    beacon period 300, range 60; multicast buffer 45, rate 200;
    RX SOP -80; CCA threshold -77
AP0022.9090.bb3e 00:24:97:88:c5:d0
    beacon period 300, range 0; multicast buffer 0, rate 0;
    RX SOP -80; CCA threshold -0
ironRap.ddbf 00:17:df:36:dd:b0
    beacon period 300, range 0; multicast buffer 0, rate 0;
    RX SOP  -80; CCA threshold -0
```

次に、無線の拡張設定および Rx SOP しきい値を表示する例を示します。

```
(Cisco Controller) > show 802.11a extended
Default 802.11a band Radio Extended Configurations:
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
    RX SOP threshold: -76; CCA threshold: 0 (AUTO);

AP3600-XALE3  34:a8:4e:6a:7b:00
    Beacon period: 100, range: 0 (AUTO);
    Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
```

```
RX SOP threshold: -76; CCA threshold: 0 (AUTO);
```

show 802.11 media-stream

マルチキャスト ダイレクト設定の状態を表示するには、**show 802.11 media-stream** コマンドを使用します。

show 802.11 {**a** | **b** | **h**} **media-stream** *media_stream_name*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
h	802.11h ネットワークを指定します。
media_stream_name	指定されたメディア ストリーム名。

コマンド デフォルト

なし。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、メディア ストリームの設定を表示する例を示します。

```
> show 802.11a media-stream rrc
Multicast-direct................................ Enabled
Best Effort..................................... Disabled
Video Re-Direct................................. Enabled
Max Allowed Streams Per Radio.................. Auto
Max Allowed Streams Per Client................. Auto
Max Video Bandwidth............................ 0
Max Voice Bandwidth............................ 75
Max Media Bandwidth............................ 85
Min PHY Rate................................... 6000
Max Retry Percentage........................... 80
```

関連コマンド

show media-stream group summary

show コマンド：a ～ i

- show aaa auth （1408 ページ）
- show acl （1409 ページ）
- show acl detailed （1411 ページ）
- show acl summary （1412 ページ）
- show advanced 802.11 channel （1413 ページ）
- show advanced 802.11 coverage （1414 ページ）
- show advanced 802.11 group （1415 ページ）
- show advanced 802.11 l2roam （1416 ページ）
- show advanced 802.11 logging （1417 ページ）
- show advanced 802.11 monitor （1418 ページ）
- show advanced 802.11 optimized roaming （1419 ページ）
- show advanced 802.11 profile （1420 ページ）
- show advanced 802.11 receiver （1421 ページ）
- show advanced 802.11 summary （1422 ページ）
- show advanced 802.11 txpower （1423 ページ）
- show advanced backup-controller （1424 ページ）
- show advanced dot11-padding （1425 ページ）
- show advanced hotspot （1426 ページ）
- show advanced max-1x-sessions （1427 ページ）
- show advanced probe （1428 ページ）
- show advanced rate （1429 ページ）
- show advanced timers （1430 ページ）
- show advanced client-handoff （1431 ページ）
- show advanced eap （1432 ページ）
- show advanced send-disassoc-on-handoff （1433 ページ）
- show advanced sip-preferred-call-no （1434 ページ）
- show advanced sip-snooping-ports （1435 ページ）
- show arp kernel （1436 ページ）
- show arp switch （1437 ページ）

- show ap auto-rf （1438 ページ）
- show ap aid-audit-mode （1440 ページ）
- show ap ccx rm （1441 ページ）
- show ap cdp （1442 ページ）
- show ap channel （1444 ページ）
- show ap config （1445 ページ）
- show ap config general （1451 ページ）
- show ap config global （1452 ページ）
- show ap core-dump （1453 ページ）
- show ap crash-file （1454 ページ）
- show ap data-plane （1455 ページ）
- show ap dtls-cipher-suite （1456 ページ）
- show ap ethernet tag （1457 ページ）
- show ap eventlog （1458 ページ）
- show ap flexconnect （1459 ページ）
- show ap image （1460 ページ）
- show ap inventory （1461 ページ）
- show ap join stats detailed （1462 ページ）
- show ap join stats summary （1463 ページ）
- show ap join stats summary all （1464 ページ）
- show ap led-state （1465 ページ）
- show ap led-flash （1466 ページ）
- show ap link-encryption （1467 ページ）
- show ap max-count summary （1468 ページ）
- show ap monitor-mode summary （1469 ページ）
- show ap module summary （1470 ページ）
- show ap packet-dump status （1471 ページ）
- show ap prefer-mode stats （1472 ページ）
- show ap retransmit （1473 ページ）
- show ap stats （1474 ページ）
- show ap summary （1477 ページ）
- show ap tcp-mss-adjust （1478 ページ）
- show ap wlan （1479 ページ）
- show assisted-roaming （1480 ページ）
- show atf config （1481 ページ）
- show atf statistics ap （1482 ページ）
- show auth-list （1483 ページ）
- show avc applications （1484 ページ）
- show avc engine （1485 ページ）
- show avc profile （1486 ページ）
- show avc protocol-pack （1487 ページ）

- show avc statistics application （1488 ページ）
- show avc statistics client （1490 ページ）
- show avc statistics guest-lan （1492 ページ）
- show avc statistics remote-lan （1494 ページ）
- show avc statistics top-apps （1496 ページ）
- show avc statistics wlan （1498 ページ）
- show boot （1500 ページ）
- show band-select （1501 ページ）
- show buffers （1502 ページ）
- show cac voice stats （1504 ページ）
- show cac voice summary （1505 ページ）
- show cac video stats （1506 ページ）
- show cac video summary （1508 ページ）
- show call-control ap （1509 ページ）
- show call-control client （1514 ページ）
- show call-home summary （1515 ページ）
- show capwap reap association （1516 ページ）
- show capwap reap status （1517 ページ）
- show cdp （1518 ページ）
- show certificate compatibility （1519 ページ）
- show certificate lsc （1520 ページ）
- show certificate ssc （1521 ページ）
- show certificate summary （1522 ページ）
- show client ap （1523 ページ）
- show client calls （1524 ページ）
- show client ccx client-capability （1525 ページ）
- show client ccx frame-data （1526 ページ）
- show client ccx last-response-status （1527 ページ）
- show client ccx last-test-status （1528 ページ）
- show client ccx log-response （1529 ページ）
- show client ccx manufacturer-info （1531 ページ）
- show client ccx operating-parameters （1532 ページ）
- show client ccx profiles （1533 ページ）
- show client ccx results （1535 ページ）
- show client ccx rm （1536 ページ）
- show client ccx stats-report （1538 ページ）
- show client detail （1539 ページ）
- show client location-calibration summary （1543 ページ）
- show client roam-history （1544 ページ）
- show client summary （1545 ページ）
- show client summary guest-lan （1547 ページ）

- show client tsm （1548 ページ）
- show client username （1550 ページ）
- show client voice-diag （1551 ページ）
- show client detail （1552 ページ）
- show client location-calibration summary （1554 ページ）
- show client probing （1555 ページ）
- show client roam-history （1556 ページ）
- show client summary （1557 ページ）
- show client wlan （1559 ページ）
- show cloud-services cmx summary （1560 ページ）
- show cloud-services cmx statistics （1561 ページ）
- show coredump summary （1562 ページ）
- show country （1563 ページ）
- show country channels （1564 ページ）
- show country supported （1565 ページ）
- show cpu （1567 ページ）
- show custom-web （1568 ページ）
- show database summary （1569 ページ）
- show dhcp （1570 ページ）
- show dhcp proxy （1571 ページ）
- show dhcp timeout （1572 ページ）
- show dtls connections （1573 ページ）
- show exclusionlist （1574 ページ）
- show flexconnect acl detailed （1575 ページ）
- show flexconnect acl summary （1576 ページ）
- show flexconnect group detail （1577 ページ）
- show flexconnect group summary （1578 ページ）
- show flexconnect office-extend （1579 ページ）
- show flow exporter （1580 ページ）
- show flow monitor summary （1581 ページ）
- show guest-lan （1582 ページ）
- show icons summary （1583 ページ）
- show ike （1584 ページ）
- show interface summary （1585 ページ）
- show interface detailed （1586 ページ）
- show interface group （1589 ページ）
- show invalid-config （1591 ページ）
- show inventory （1592 ページ）
- show IPsec （1593 ページ）
- show ipv6 acl （1595 ページ）
- show ipv6 summary （1596 ページ）

- show guest-lan （1597 ページ）
- show icons file-info （1598 ページ）
- show ipv6 acl （1599 ページ）
- show ipv6 acl cpu （1600 ページ）
- show ipv6 acl detailed （1601 ページ）
- show ipv6 neighbor-binding （1602 ページ）
- show ipv6 ra-guard （1606 ページ）
- show ipv6 route summary （1607 ページ）
- show ipv6 summary （1608 ページ）
- show known ap （1609 ページ）

show aaa auth

認証、許可、アカウンティング（AAA）認証サーバのデータベースの設定を表示するには、**show aaa auth** コマンドを使用します。

show aaa auth

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、AAA 認証サーバのデータベースの設定を表示する例を示します。

```
(Cisco Controller) > show aaa auth
Management authentication server order:
    1..................................... local
    2..................................... tacacs
```

関連コマンド

config aaa auth

config aaa auth mgmt

show acl

コントローラに設定されているアクセス コントロール リスト（ACL）を表示するには、**show acl** コマンドを使用します。

show acl {**cpu** | **detailed** *acl_name* | **summary** | **layer2** { **summary** | **detailed** *acl_name* } }

構文の説明

cpu	Cisco WLC の中央処理装置（CPU）に設定されている ACL を表示します。
detailed	特定の ACL の詳細情報を表示します。
acl_name	ACL 名です。名前には 32 文字以内の英数字を使用できます。
summary	コントローラに設定されているすべての ACL の要約を表示します。
layer2	レイヤ 2 ACL を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CPU のアクセス コントロール リストを表示する例を示します。

```
(Cisco Controller) >show acl cpu

CPU Acl Name.................................
Wireless Traffic............................. Disabled
Wired Traffic................................ Disabled
Applied to NPU............................... No
```

次に、アクセス コントロール リストのサマリーを表示する例を示します。

```
(Cisco Controller) > show acl summary

ACL Counter Status               Disabled
-----------------------------------------
IPv4 ACL Name                     Applied
-------------------------------- -------
acl1                            Yes
acl2                            Yes
```

```
acl3                            Yes
---------------------------------------
IPv6 ACL Name                      Applied
--------------------------------- -------
acl6                             No
```

次に、アクセス コントロール リストの詳細情報を表示する例を示します。

```
(Cisco Controller) > show acl detailed acl_name

     Source              Destination        Source Port Dest Port
I Dir IP Address/Netmask IP
Address/Netmask Prot   Range    Range     DSCP Action Counter
- --- ------------------ ------------------ ---- --------- ---------
----- ------ -------
1
Any 0.0.0.0/0.0.0.0    0.0.0.0/0.0.0.0    Any  0-65535   0-65535    0    Deny        0
2
In  0.0.0.0/0.0.0.0    200.200.200.0/     6     80-80   0-65535    Any  Permit      0
                              255.255.255.0
DenyCounter :      0
```

（注） パケットが ACL ルールと一致するたびに、Counter フィールドの値が増加します。また、DenyCounterフィールドの値は、パケットがルールのいずれとも一致しない場合に増加します。

関連コマンド

clear acl counters

config acl apply

config acl counter

config acl cpu

config acl create

config acl delete

config interface acl

config acl rule

show acl detailed

DNS ベースの詳細な ACL 情報を表示するには、**show acl detailed** コマンドを使用します。

show acl detailed*acl_name*

構文の説明

acl_name	アクセス コントロール リストの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。

次に、**show acl detailed** *acl_name* コマンドの出力例を示します。

```
(Cisco Controller) > show acl detailed android

No rules are configured for this ACL.
DenyCounter : 0
URLs configured in this ACL
---------------------------
*.play.google.com
*.store.google.com
```

show acl summary

DNS ベースの ACL 情報を表示するには、**show acl summary** コマンドを使用します。

show aclsummary

構文の説明

summary	DNS ベースの ACL 情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show acl summary** コマンドの出力例を示します。

```
(Cisco Controller) > show acl summary

 ACL Counter Status               Disabled
--------------------------------------
IPv4 ACL Name                     Applied
--------------------------------- -------
android                           No
StoreACL                          Yes
--------------------------------------
IPv6 ACL Name                     Applied
--------------------------------- -------                    1
```

show advanced 802.11 channel

自動チャネル割り当ての設定と統計情報を表示するには、**show advanced 802.11 channel** コマンドを使用します。

show advanced 802.11{**a** | **b**} **channel**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、自動チャネル割り当ての設定および統計情報を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11a channel
Automatic Channel Assignment
  Channel Assignment Mode..................... AUTO
  Channel Update Interval..................... 600 seconds [startup]

  Anchor time (Hour of the day)................ 0
  Channel Update Contribution.................. SNI.
  Channel Assignment Leader.................... 00:1a:6d:dd:1e:40
  Last Run..................................... 129 seconds ago
  DCA Sensitivity Level: ..................... STARTUP (5 dB)
  DCA Minimum Energy Limit..................... -95 dBm
Channel Energy Levels
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Channel Dwell Times
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Auto-RF Allowed Channel List...................
36,40,44,48,52,56,60,64,149,
    ............................................ 153,157,161
  Auto-RF Unused Channel List...................
100,104,108,112,116,132,136,
    ............................................ 140,165,190,196
  DCA Outdoor AP option........................ Enabled
```

show advanced 802.11 coverage

カバレッジ ホール検出の設定と統計情報を表示するには、**show advanced 802.11 coverage** コマンドを使用します。

show advanced 802.11{**a** | **b**} **coverage**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、カバレッジ ホール検出の統計情報を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11a coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode..... Enabled
  802.11a Coverage Voice Packet Count..... 100 packets
  802.11a Coverage Voice Packet Percentage..... 50%
  802.11a Coverage Voice RSSI Threshold..... -80 dBm
  802.11a Coverage Data Packet Count..... 50 packets
  802.11a Coverage Data Packet Percentage..... 50%
  802.11a Coverage Data RSSI Threshold..... -80 dBm
  802.11a Global coverage exception level..... 25 %
  802.11a Global client minimum exception lev.... 3 clients
```

show advanced 802.11 group

シスコの 802.11a または 802.11b 対応無線の無線周波数（RF）グループ化を表示するには、**show advanced 802.11 group** コマンドを使用します。

show advanced 802.11{**a** | **b**} **group**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、シスコの無線 RF グループ設定を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11a group
Radio RF Grouping
  802.11a Group Mode..................................... AUTO
  802.11a Group Update Interval.......................... 600 seconds
  802.11a Group Leader................................... xx:xx:xx:xx:xx:xx
    802.11a Group Member................................. xx:xx:xx:xx:xx:xx
  802.11a Last Run....................................... 133 seconds ago
```

show advanced 802.11 l2roam

802.11a または 802.11b/g レイヤ 2 クライアントのローミング情報を表示するには、**show advanced 802.11 l2roam** コマンドを使用します。

show advanced 802.11{**a** | **b**} **l2roam** {**rf-param** | **statistics**} *mac_address*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
rf-param	レイヤ 2 周波数パラメータを指定します。
statistics	レイヤ 2 クライアントのローミング統計情報を指定します。
mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show advanced 802.11b l2roam rf-param** コマンドの出力例を示します。

```
(Cisco Controller) > show advanced 802.11b l2roam rf-param

L2Roam 802.11bg RF Parameters.....................
    Config Mode................................. Default
    Minimum RSSI................................ -85
    Roam Hysteresis............................. 2
    Scan Threshold.............................. -72
    Transition time............................. 5
```

show advanced 802.11 logging

802.11a または 802.11b の RF イベント ログおよびパフォーマンス ログを表示するには、**show advanced 802.11 logging** コマンドを使用します。

show advanced 802.11{**a** | **b**} **logging**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11b RF イベント ログおよびパフォーマンス ログを表示する例を示します。

```
(Cisco Controller) > show advanced 802.11b logging
RF Event and Performance Logging
  Channel Update Logging..... Off
  Coverage Profile Logging..... Off
  Foreign Profile Logging..... Off
  Load Profile Logging..... Off
  Noise Profile Logging..... Off
  Performance Profile Logging..... Off
  TxPower Update Logging..... Off
```

show advanced 802.11 monitor

デフォルトのシスコの 802.11a または 802.11b 対応無線監視を表示するには、**show advanced 802.11 monitor** コマンドを使用します。

show advanced 802.11{**a** | **b**} **monitor**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11b ネットワークの無線監視を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11b monitor
Default 802.11b AP monitoring
  802.11b Monitor Mode..................................... enable
  802.11b Monitor Channels................................. Country channels
  802.11b RRM Neighbor Discovery Type...................... Transparent
  802.11b AP Coverage Interval............................. 180 seconds
  802.11b AP Load Interval................................. 60 seconds
  802.11b AP Noise Interval................................ 180 seconds
  802.11b AP Signal Strength Interval...................... 60 seconds
```

show advanced 802.11 optimized roaming

802.11 a/b ネットワークの最適化されたローミング設定を表示するには、**show advanced 802.11 optimized roaming** コマンドを使用します。

show advanced 802.11 {**a** | **b**} **optimized roaming** [**stats**]

構文の説明

stats	（任意）802.11a/b ネットワークの最適化されたローミング統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、802.11a ネットワークの最適化されたローミング設定を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11a optimized roaming
OptimizedRoaming
  802.11a OptimizedRoaming Mode.................. Enabled
  802.11a OptimizedRoaming Reporting Interval.... 20 seconds
  802.11a OptimizedRoaming Rate Threshold........ disabled
```

次に、802.11a ネットワークの最適化されたローミング統計情報を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11a optimized roaming stats
OptimizedRoaming Stats
802.11a OptimizedRoaming Disassociations....... 2
802.11a OptimizedRoaming Rejections............ 1
```

show advanced 802.11 profile

802.11a または 802.11b 対応 Lightweight アクセス ポイントのパフォーマンス プロファイルを表示するには、**show advanced 802.11 profile** コマンドを使用します。

show advanced 802.11{**a** | **b**} **profile** {**global** | *cisco_ap* }

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての Cisco Lightweight アクセス ポイントを指定します。
cisco_ap	特定の Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11a プロファイルのグローバル設定と統計情報を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11 profile global
Default 802.11a AP performance profiles
  802.11a Global Interference threshold.............. 10%
  802.11a Global noise threshold..................... -70 dBm
  802.11a Global RF utilization threshold............ 80%
  802.11a Global throughput threshold................ 1000000 bps
  802.11a Global clients threshold................... 12 clients
  802.11a Global coverage threshold.................. 12 dB
  802.11a Global coverage exception level............ 80%
  802.11a Global client minimum exception lev........ 3 clients
```

次に、特定のアクセス ポイント プロファイルの設定と統計情報を表示する例を示します。

```
(Cisco Controller) >  show advanced 802.11 profile AP1
Cisco AP performance profile not customized
```

この応答は、この Lightweight アクセス ポイントのパフォーマンス プロファイルがグローバルなデフォルト設定を使用しており、個別に設定されていないことを示しています。

show advanced 802.11 receiver

802.11a または 802.11b レシーバの設定と統計情報を表示するには、**show advanced 802.11 receiver** コマンドを使用します。

show advanced 802.11 {**a** | **b**} **receiver**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11a ネットワークの設定および統計情報を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11 receiver
802.11a Receiver Settings
  RxStart   : Signal Threshold.......................... 15
  RxStart   : Signal Lamp Threshold..................... 5
  RxStart   : Preamble Power Threshold.................. 2
  RxReStart : Signal Jump Status........................ Enabled
  RxReStart : Signal Jump Threshold..................... 10
  TxStomp : Low RSSI Status............................. Enabled
  TxStomp : Low RSSI Threshold.......................... 30
  TxStomp : Wrong BSSID Status.......................... Enabled
  TxStomp : Wrong BSSID Data Only Status................ Enabled
  RxAbort : Raw Power Drop Status....................... Disabled
  RxAbort : Raw Power Drop Threshold.................... 10
  RxAbort : Low RSSI Status............................. Disabled
  RxAbort : Low RSSI Threshold.......................... 0
  RxAbort : Wrong BSSID Status.......................... Disabled
  RxAbort : Wrong BSSID Data Only Status................ Disabled
```

show advanced 802.11 summary

802.11a または 802.11b の Cisco Lightweight アクセス ポイントの名前、チャネル、および送信レベルのサマリーを表示するには、**show advanced 802.11 summary** コマンドを使用します。

show advanced 802.11{**a** | **b**} **summary**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11b アクセス ポイント設定の要約を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11b summary
AP Name      MAC Address         Admin State  Operation State   Channel
 TxPower
------------ ------------------ ------------ ----------------- -------
 --------
CJ-1240      00:21:1b:ea:36:60    ENABLED          UP           161
   1( )
CJ-1130      00:1f:ca:cf:b6:60    ENABLED          UP           56*
   1(*)
```

（注） チャネル番号または伝送レベルの横のアスタリスク（*）は、グローバルなアルゴリズム設定によって制御されていることを示します。

show advanced 802.11 txpower

802.11a または 802.11b 自動伝送パワー割り当てを表示するには、**show advanced 802.11 txpower** コマンドを使用します。

show advanced 802.11 {**a** | **b**} **txpower**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、802.11b 伝送パワー コストの設定および統計情報を表示する例を示します。

```
(Cisco Controller) > show advanced 802.11b txpower
Automatic Transmit Power Assignment
  Transmit Power Assignment Mode..................... AUTO
  Transmit Power Update Interval..................... 600 seconds
  Transmit Power Threshold........................... -65 dBm
  Transmit Power Neighbor Count...................... 3 APs
  Transmit Power Update Contribution................. SN.
  Transmit Power Assignment Leader................... xx:xx:xx:xx:xx:xx
  Last Run........................................... 384 seconds ago
```

show advanced backup-controller

プライマリおよびセカンダリ バックアップ WLC のリストを表示するには、**show advanced backup-controller** コマンドを使用します。

show advanced backup-controller

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、バックアップ コントローラ情報を表示する例を示します。

```
(Cisco Controller) >
show advanced backup-controller
AP primary Backup Controller .....................  controller 10.10.10.10
AP secondary Backup Controller ...................  0.0.0.0
```

show advanced dot11-padding

Wireless LAN Controller の無線フレーム パディングの状態を表示するには、**show advanced dot11-padding** コマンドを使用します。

show advanced dot11-padding

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、無線フレーム パディングの状態を表示する例を示します。

```
(Cisco Controller) > show advanced dot11-padding
dot11-padding..................................... Disabled
```

show advanced hotspot

詳細なホットスポット パラメータを表示するには、**show advanced hotspot** コマンドを使用します。

show advanced hotspot

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、詳細なホットスポット パラメータを表示する例を示します。

```
(Cisco Controller) >show advanced hotspot
ANQP 4-way state.............................. Disabled
GARP Broadcast state: ........................ Enabled
GAS request rate limit ....................... Disabled
ANQP comeback delay in TUs(TU=1024usec)..... 50
```

show advanced max-1x-sessions

各アクセス ポイントに許可されている同時 802.1X セッションの最大数を表示するには、**show advanced max-1x-sessions** コマンドを使用します。

show advanced max-1x-sessions

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、各アクセス ポイントの最大 802.1X セッションを表示する例を示します。

```
(Cisco Controller) >show advanced max-1x-sessions
Max 802.1x session per AP at a given time........ 0
```

show advanced probe

各クライアントのアクセス ポイント当たりの Cisco WLC に送信されたプローブ数およびプローブ間隔（ミリ秒）を表示するには、**show advanced probe** コマンドを使用します。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、WLAN コントローラのプローブ設定を表示する例を示します。

```
(Cisco Controller) >show advanced probe
Probe request filtering..................... Enabled
Probes fwd to controller per client per radio.... 12
Probe request rate-limiting interval..... 100 msec
```

show advanced rate

制御パス レート制限が有効か無効かを表示するには、**show advanced rate** コマンドを使用します。

show advanced rate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、スイッチの制御パス レート制限モードを表示する例を示します。

```
(Cisco Controller) >show advanced rate
Control Path Rate Limiting.....................  Disabled
```

show advanced timers

モビリティ アンカー、認証応答、および不正なアクセス ポイントのエントリ タイマーを表示するには、**show advanced timers** コマンドを使用します。

show advanced timers

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトは「例」に記載されています。

次に、システム タイマーの設定を表示する例を示します。

```
(Cisco Controller) >show advanced timers
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds)..................... 1200
AP Heart Beat Timeout (seconds)................... 30
AP Discovery Timeout (seconds).................... 10
AP Local mode Fast Heartbeat (seconds)............ disable
AP flexconnect mode Fast Heartbeat (seconds)...... disable
AP Primary Discovery Timeout (seconds)........... 120
```

show advanced client-handoff

再試行後の自動クライアント ハンドオフ回数を表示するには、**show advanced client-handoff** コマンドを使用します。

show advanced client-handoff

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、再試行数の上限を超えた後に、クライアントの自動ハンドオフ モードを表示する例を示します。

```
(Cisco Controller) >show advanced client-handoff
Client auto handoff after retries.............  130
```

show advanced eap

拡張認証プロトコル（EAP）設定を表示するには、**show advanced eap** コマンドを使用します。

show advanced eap

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、EAP 設定を表示する例を示します。

```
(Cisco Controller) > show advanced eap
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries.............. 20
EAP Key-Index for Dynamic WEP................. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)................. 1
EAP-Request Max Retries....................... 20
EAPOL-Key Timeout (milliseconds).............. 1000
EAPOL-Key Max Retries......................... 2
```

関連コマンド

config advanced eap

config advanced timers eap-identity-request-delay

config advanced timers eap-timeout

show advanced send-disassoc-on-handoff

ハンドオフ後に WLAN コントローラがクライアントをアソシエート解除するかどうかを表示するには、**show advanced send-disassoc-on-handoff** コマンドを使用します。

show advanced send-disassoc-on-handoff

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show advanced send-disassoc-on-handoff** コマンドの出力例を示します。

```
(Cisco Controller) > show advanced send-disassoc-on-handoff
Send Disassociate on Handoff..................... Disabled
```

show advanced sip-preferred-call-no

優先コール番号のリストを表示するには、**show advanced sip-preferred-call-no** コマンドを使用します。

show advanced sip-preferred-call-no

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show advanced sip-preferred-call-no** コマンドの出力例を示します。

```
(Cisco Controller) > show advanced sip-preferred-call-no
Preferred Call Numbers List
Call Index            Preferred Call No
-----------           -------------------
1                      911
2                      100
3                      101
4                      102
5                      103
6                      104
```

show advanced sip-snooping-ports

コールスヌーピングのポート範囲を表示するには、**show advanced sip-snooping-ports** コマンドを使用します。

show advanced sip-snooping-ports

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show advanced sip-snooping-ports** コマンドの出力例を示します。

```
(Cisco Controller) > show advanced sip-snooping-ports
 SIP Call Snoop Ports: 1000 - 2000
```

show arp kernel

カーネルアドレス解決プロトコル（ARP）のキャッシュ情報を表示するには、**show arp kernel** コマンドを使用します。

show arp kernel

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show arp kernel** コマンドの出力例を示します。

```
(Cisco Controller) > show arp kernel
IP address       HW type     Flags       HW address            Mask     Device
192.0.2.1        0x1         0x2         00:1A:6C:2A:09:C2     *        dtl0
192.0.2.8        0x1         0x6         00:1E:E5:E6:DB:56     *        dtl0
```

show arp switch

Cisco Wireless LAN Controller の MAC アドレス、IP アドレス、およびポート タイプを表示するには、**show arp switch** コマンドを使用します。

show arp switch

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show arp switch** コマンドの出力例を示します。

```
(Cisco Controller) > show arp switch
MAC Address          IP Address         Port      VLAN      Type
-------------------- ---------------- ------------ ---- --------------------
xx:xx:xx:xx:xx:xx   xxx.xxx.xxx.xxx  service port    1
xx:xx:xx:xx:xx:xx   xxx.xxx.xxx.xxx  service port
xx:xx:xx:xx:xx:xx   xxx.xxx.xxx.xxx  service port
```

show ap auto-rf

Cisco Lightweight アクセス ポイントの自動 RF 設定を表示するには、**show ap auto-rf** コマンドを使用します。

show ap auto-rf 802.11{**a** | **b**} *cisco_ap*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、アクセス ポイントの自動 RF 情報を表示する例を示します。

```
(Cisco Controller) > show ap auto-rf 802.11a AP1
Number Of Slots..................................... 2
AP Name............................................. AP03
MAC Address......................................... 00:0b:85:01:18:b7
  Radio Type........................................ RADIO_TYPE_80211a
  Noise Information
    Noise Profile................................... PASSED
    Channel 36.....................................  -88 dBm
    Channel 40.....................................  -86 dBm
    Channel 44.....................................  -87 dBm
    Channel 48.....................................  -85 dBm
    Channel 52.....................................  -84 dBm
    Channel 56.....................................  -83 dBm
    Channel 60.....................................  -84 dBm
    Channel 64.....................................  -85 dBm
  Interference Information
    Interference Profile............................ PASSED
    Channel 36.....................................  -66 dBm @  1% busy
    Channel 40..................................... -128 dBm @  0% busy
    Channel 44..................................... -128 dBm @  0% busy
    Channel 48..................................... -128 dBm @  0% busy
    Channel 52..................................... -128 dBm @  0% busy
    Channel 56.....................................  -73 dBm @  1% busy
    Channel 60.....................................  -55 dBm @  1% busy
    Channel 64.....................................  -69 dBm @  1% busy
  Rogue Histogram (20/40_ABOVE/40_BELOW)
    Channel 36..................................... 16/ 0/ 0
    Channel 40..................................... 28/ 0/ 0
    Channel 44.....................................  9/ 0/ 0
    Channel 48.....................................  9/ 0/ 0
    Channel 52.....................................  3/ 0/ 0
    Channel 56.....................................  4/ 0/ 0
```

```
  Channel 60.................................  7/ 1/ 0
  Channel 64.................................  2/ 0/ 0
Load Information
  Load Profile.............................. PASSED
  Receive Utilization....................... 0%
  Transmit Utilization...................... 0%
  Channel Utilization....................... 1%
  Attached Clients.......................... 1 clients
Coverage Information
  Coverage Profile.......................... PASSED
  Failed Clients............................ 0 clients
Client Signal Strengths
  RSSI -100 dBm............................. 0 clients
  RSSI  -92 dBm............................. 0 clients
  RSSI  -84 dBm............................. 0 clients
  RSSI  -76 dBm............................. 0 clients
  RSSI  -68 dBm............................. 0 clients
  RSSI  -60 dBm............................. 0 clients
  RSSI  -52 dBm............................. 0 clients
Client Signal To Noise Ratios
  SNR    0 dBm.............................. 0 clients
  SNR    5 dBm.............................. 0 clients
  SNR   10 dBm.............................. 0 clients
  SNR   15 dBm.............................. 0 clients
  SNR   20 dBm.............................. 0 clients
  SNR   25 dBm.............................. 0 clients
  SNR   30 dBm.............................. 0 clients
  SNR   35 dBm.............................. 0 clients
  SNR   40 dBm.............................. 0 clients
  SNR   45 dBm.............................. 0 clients
Nearby RADs
  RAD 00:0b:85:01:05:08 slot 0.............. -46 dBm on 10.1.30.170
  RAD 00:0b:85:01:12:65 slot 0.............. -24 dBm on 10.1.30.170
Channel Assignment Information
  Current Channel Average Energy.............. -86 dBm
  Previous Channel Average Energy............. -75 dBm
  Channel Change Count........................ 109
  Last Channel Change Time.................... Wed Sep 29 12:53e:34
2004
  Recommended Best Channel.................... 44
RF Parameter Recommendations
  Power Level............................... 1
  RTS/CTS Threshold......................... 2347
  Fragmentation Threshold................... 2346
  Antenna Pattern........................... 0
```

show ap aid-audit-mode

AP で AID 監査モードのステータスを表示するには、**show ap aid-audit mode** コマンドを使用します。

show ap aid-audit mode

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.6	このコマンドが導入されました。

次に、AID 監査モードのステータスを表示する例を示します。

```
(Cisco Controller) > show ap aid-audit-mode
 Aid Audit Mode ................................ Disabled
```

show ap ccx rm

アクセス ポイントの Cisco Client Extension（CCX）無線管理ステータス情報を表示するには、**show ap ccx rm** コマンドを使用します。

show ap ccx rm *ap_name* **status**

構文の説明

ap_name	特定のアクセス ポイント名。
status	アクセス ポイントの CCX 無線管理ステータス情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、CCX 無線管理のステータスを表示する例を示します。

```
(Cisco Controller) >show ap ccx rm AP1240-21ac status
A Radio
Channel Load Request ..................... Disabled
Noise Histogram Request .................. Disabled
Beacon Request ........................... Disabled
Frame Request ............................ Disabled
Interval ................................. 60
Iteration ................................ 10
G Radio
Channel Load Request ..................... Disabled
Noise Histogram Request .................. Disabled
Beacon Request ........................... Disabled
Frame Request ............................ Disabled
Interval ................................. 60
Iteration ................................ 10
```

show ap cdp

アクセス ポイントの Cisco Discovery Protocol（CDP）情報を表示するには、**show ap cdp** コマンドを使用します。

show ap cdp {**all** | **ap-name** *cisco_ap* | **neighbors** {**all** | **ap-name** *cisco_ap* | **detail** *cisco_ap*}}

構文の説明

all	すべてのアクセスポイントのCDPステータスを表示します。
ap-name	特定のアクセスポイントのCDPステータスを表示します。
cisco_ap	特定のアクセス ポイント名。
neighbors	CDP を使用してネイバーを表示します。
detail	CDP を使用する特定のアクセス ポイントのネイバーに関する情報を表示します。

コマンド デフォルト

なし

次に、すべてのアクセス ポイントの CDP ステータスを表示する例を示します。

```
(Cisco Controller) >show ap cdp all
AP CDP State
AP Name             AP CDP State
------------------  ----------
SB_RAP1              enable
SB_MAP1              enable
SB_MAP2              enable
SB_MAP3              enable
```

次に、指定したアクセス ポイントの CDP ステータスを表示する例を示します。

```
(Cisco Controller) >show ap cdp ap-name SB_RAP1
AP CDP State
AP Name             AP CDP State
------------------  ----------
AP CDP State.....................Enabled
AP Interface-Based CDP state
 Ethernet 0.....................Enabled
 Slot 0.........................Enabled
 Slot 1.........................Enabled
```

次に、CDP を使用するすべてのネイバーの詳細を表示する例を示します。

```
(Cisco Controller) >show ap cdp neighbor all
AP Name     AP IP            Neighbor Name       Neighbor IP      Neighbor Port
```

```
---------   ---------------  ------------------  --------------  -------------
SB_RAP1     192.168.102.154  sjc14-41a-sw1       192.168.102.2    GigabitEthernet1/0/13
SB_RAP1     192.168.102.154  SB_MAP1             192.168.102.137  Virtual-Dot11Radio0
SB_MAP1     192.168.102.137  SB_RAP1             192.168.102.154  Virtual-Dot11Radio0
SB_MAP1     192.168.102.137  SB_MAP2             192.168.102.138  Virtual-Dot11Radio0
SB_MAP2     192.168.102.138  SB_MAP1             192.168.102.137  Virtual-Dot11Radio1
SB_MAP2     192.168.102.138  SB_MAP3             192.168.102.139  Virtual-Dot11Radio0
SB_MAP3     192.168.102.139  SB_MAP2             192.168.102.138  Virtual-Dot11Radio1
```

次に、CDPを使用して指定したアクセスポイントを持つ特定のネイバーの詳細を表示する例を示します。

```
(Cisco Controller) >show ap cdp neighbors ap-name SB_MAP2
AP Name      AP IP            Neighbor Name    Neighbor IP      Neighbor Port
-----------  ---------------  ---------------  --------------  -------------
SB_MAP2      192.168.102.138  SB_MAP1          192.168.102.137  Virtual-Dot11Radio1
SB_MAP2      192.168.102.138  SB_MAP3          192.168.102.139  Virtual-Dot11Radio0
```

次に、CDP を使用するネイバーの詳細を表示する例を示します。

```
(Cisco Controller) >show ap cdp neighbors detail SB_MAP2
AP Name:SB_MAP2
AP IP address:192.168.102.138
-------------------------
Device ID: SB_MAP1
Entry address(es): 192.168.102.137
Platform: cisco AIR-LAP1522AG-A-K9  ,  Cap
Interface: Virtual-Dot11Radio0,  Port ID (outgoing port): Virtual-Dot11Radio1
Holdtime : 180 sec
Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(200
81114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by
 Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by
advertisement version: 2
-------------------------
Device ID: SB_MAP3
Entry address(es): 192.168.102.139
Platform: cisco AIR-LAP1522AG-A-K9  ,  Capabilities: Trans-Bridge
Interface: Virtual-Dot11Radio1,  Port ID (outgoing port): Virtual-Dot11Radio0
Holdtime : 180 sec
Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(200
81114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by
 Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by
advertisement version: 2
```

show ap channel

特定のメッシュ アクセス ポイントの使用可能なチャネルを表示するには、**show ap channel** コマンドを使用します。

show ap channel *ap_name*

構文の説明

ap_name	メッシュ アクセス ポイントの名前。

コマンド デフォルト

なし

次に、特定のアクセス ポイントの使用可能なチャネルを表示する例を示します。

```
(Cisco Controller) >show ap channel AP47
 802.11b/g Current Channel ...........1
Allowed Channel List.....................1,2,3,4,5,6,7,8,9,10,11
802.11a Current Channel ..................161
Allowed Channel List.....................36,40,44,48,52,56,60,64,100,
.........................................104,108,112,116,132,136,140,
.........................................149,153,157,161
```

show ap config

Lightweight アクセス ポイントの詳細設定を表示するには、**show ap config** コマンドを使用します。

show ap config 802.11{**a** | **b**} [**summary**] *cisco_ap*

構文の説明

802.11a	802.11a または 802.11b/g ネットワークを指定します。
802.11b	802.11b/g ネットワークを指定します。
summary	（任意）すべての AP の無線サマリーを表示します。
cisco_ap	Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

次に、アクセス ポイントの詳細設定を表示する例を示します。

```
(Cisco Controller) >show ap config 802.11a AP02
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... AP02
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Regulatory Domain............................. Unconfigured
Switch Port Number .............................. 1
MAC Address...................................... 00:0b:85:18:b6:50
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.49.240
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 1.100.49.1
CAPWAP Path MTU.................................. 1485
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default-location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. Cisco_32:ab:63
Primary Cisco Switch IP Address.................. Not Configured
Secondary Cisco Switch...........................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch............................
Tertiary Cisco Switch IP Address................. Not Configured
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Sniffer
Public Safety ................................... Global: Disabled, Local: Disabled
AP SubMode ...................................... Not Configured
Remote AP Debug ................................. Disabled
Logging trap severity level ..................... informational
Logging syslog facility ......................... kern
S/W  Version .................................... 7.0.110.6
```

```
Boot  Version ................................... 12.4.18.0
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
Stats Re--More-- or (q)uit
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Disabled
Power Type/Mode.................................. Power injector / Normal mode
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1142N-A-K9
AP Image......................................... C1140-K9W8-M
IOS Version...................................... 12.4(20100502:031212)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1305S180
AP Certificate Type.............................. Manufacture Installed
AP User Mode..................................... AUTOMATIC
AP User Name..................................... Not Configured
AP Dot1x User Mode............................... Not Configured
AP Dot1x User Name............................... Not Configured
Cisco AP system logging host..................... 255.255.255.255
AP Up Time....................................... 47 days, 23 h 47 m 47 s
AP LWAPP Up Time................................. 47 days, 23 h 10 m 37 s
Join Date and Time............................... Tue May  4 16:05:00 2010
Join Taken Time.................................. 0 days, 00 h 01 m 37 s
Attributes for Slot  1
    Radio Type................................... RADIO_TYPE_80211n-5
    Radio Subband................................ RADIO_SUBBAND_ALL
    Administrative State ........................ ADMIN_ENABLED
    Operation State ............................. UP
    Radio Role .................................. ACCESS
    CellId ...................................... 0
Station Configuration
      Configuration ............................. AUTOMATIC
      Number Of WLANs ........................... 2
      Medium Occupancy Limit .................... 100
      CFP Period ................................ 4
      CFP MaxDuration ........................... 60
      BSSID ..................................... 00:24:97:88:99:60
Operation Rate Set
        6000 Kilo Bits........................... MANDATORY
        9000 Kilo Bits........................... SUPPORTED
        12000 Kilo Bits.......................... MANDATORY
        18000 Kilo Bits.......................... SUPPORTED
        24000 Kilo Bits.......................... MANDATORY
        36000 Kilo Bits.......................... SUPPORTED
        48000 Kilo Bits.......................... SUPPORTED
        54000 Kilo Bits.......................... SUPPORTED
      MCS Set
        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
```

```
      Beacon Period ............................. 100
      Fragmentation Threshold ................... 2346
      Multi Domain Capability Implemented ....... TRUE
      Multi Domain Capability Enabled ........... TRUE
      Country String ............................ US
Multi Domain Capability
      Configuration ............................. AUTOMATIC
      First Chan Num ............................ 36
      Number Of Channels ........................ 21
MAC Operation Parameters
      Configuration ............................. AUTOMATIC
      Fragmentation Threshold ................... 2346
      Packet Retry Limit ........................ 64
Tx Power
      Num Of Supported Power Levels ............. 6
      Tx Power Level 1 .......................... 14 dBm
      Tx Power Level 2 .......................... 11 dBm
      Tx Power Level 3 .......................... 8 dBm
      Tx Power Level 4 .......................... 5 dBm
      Tx Power Level 5 .......................... 2 dBm
      Tx Power Level 6 .......................... -1 dBm
      Tx Power Configuration .................... AUTOMATIC
      Current Tx Power Level .................... 0
Phy OFDM parameters
      Configuration ............................. AUTOMATIC
      Current Channel ........................... 36
      Extension Channel ......................... NONE
      Channel Width.............................. 20 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 .............................. -50
      Legacy Tx Beamforming Configuration ....... AUTOMATIC
      Legacy Tx Beamforming ..................... DISABLED
      Antenna Type............................... INTERNAL_ANTENNA
      Internal Antenna Gain (in .5 dBi units).... 6
      Diversity.................................. DIVERSITY_ENABLED
      802.11n Antennas
        Tx
         A....................................... ENABLED
         B....................................... ENABLED
        Rx
         A....................................... ENABLED
         B....................................... ENABLED
         C....................................... ENABLED
Performance Profile Parameters
      Configuration ............................. AUTOMATIC
      Interference threshold..................... 10 %
      Noise threshold............................  -70 dBm
      RF utilization threshold................... 80 %
      Data-rate threshold........................ 1000000 bps
      Client threshold........................... 12 clients
      Coverage SNR threshold..................... 16 dB
      Coverage exception level................... 25 %
      Client minimum exception level............. 3 clients
Rogue Containment Information
    Containment Count............................ 0
CleanAir Management Information
        CleanAir Capable......................... No
Radio Extended Configurations:
        Buffer size ……..30
        Data-rate……..0
        Beacon strt ……..90 ms
       Rx-Sensitivity SOP threshold …….. -80 dB
```

```
        CCA threshold ..... -60 dB
```

次に、別のアクセス ポイントの詳細設定を表示する例を示します。

```
(Cisco Controller) >show ap config 802.11b AP02
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... AP02
AP Regulatory Domain............................. Unconfigured
Switch Port Number .............................. 1
MAC Address...................................... 00:0b:85:18:b6:50
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.49.240
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 1.100.49.1
Cisco AP Location................................ default-location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. Cisco_32:ab:63
Secondary Cisco Switch.....................
Tertiary Cisco Switch.....................
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Remote AP Debug ................................. Disabled
S/W  Version .................................... 3.1.61.0
Boot  Version ................................... 1.2.59.6
Stats Reporting Period .......................... 180
LED State........................................ Enabled
ILP Pre Standard Switch.......................... Disabled
ILP Power Injector............................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AS-1200
AP Serial Number................................. 044110223A
AP Certificate Type.............................. Manufacture Installed
Attributes for Slot  1
    Radio Type................................... RADIO_TYPE_80211g
    Administrative State ........................ ADMIN_ENABLED
    Operation State ............................. UP
    CellId ...................................... 0
    Station Configuration
      Configuration ............................. AUTOMATIC
      Number Of WLANs ........................... 1
      Medium Occupancy Limit .................... 100
      CFP Period ................................ 4
      CFP MaxDuration ........................... 60
      BSSID ..................................... 00:0b:85:18:b6:50
      Operation Rate Set
        1000 Kilo Bits........................... MANDATORY
        2000 Kilo Bits........................... MANDATORY
        5500 Kilo Bits........................... MANDATORY
        11000 Kilo Bits.......................... MANDATORY
        6000 Kilo Bits........................... SUPPORTED
        9000 Kilo Bits........................... SUPPORTED
        12000 Kilo Bits.......................... SUPPORTED
        18000 Kilo Bits.......................... SUPPORTED
        24000 Kilo Bits.......................... SUPPORTED
        36000 Kilo Bits.......................... SUPPORTED
        48000 Kilo Bits.......................... SUPPORTED
        54000 Kilo Bits.......................... SUPPORTED
      Beacon Period ............................. 100
      DTIM Period ............................... 1
      Fragmentation Threshold ................... 2346
```

```
  Multi Domain Capability Implemented ..... TRUE
  Multi Domain Capability Enabled ..... TRUE
  Country String ..... US
Multi Domain Capability
  Configuration ..... AUTOMATIC
  First Chan Num ..... 1
  Number Of Channels ..... 11
MAC Operation Parameters
  Configuration ..... AUTOMATIC
  RTS Threshold ..... 2347
  Short Retry Limit ..... 7
  Long Retry Limit ..... 4
  Fragmentation Threshold ..... 2346
  Maximum Tx MSDU Life Time ..... 512
  Maximum Rx Life Time..... 512
Tx Power
  Num Of Supported Power Levels..... 5
  Tx Power Level 1 ..... 17 dBm
  Tx Power Level 2..... 14 dBm
  Tx Power Level 3..... 11 dBm
  Tx Power Level 4..... 8 dBm
  Tx Power Level 5..... 5 dBm
  Tx Power Configuration..... CUSTOMIZED
  Current Tx Power Level..... 5
Phy OFDM parameters
  Configuration..... CUSTOMIZED
  Current Channel..... 1
  TI Threshold..... -50
  Legacy Tx Beamforming Configuration ..... CUSTOMIZED
  Legacy Tx Beamforming ..... ENABLED
  Antenna Type..... INTERNAL_ANTENNA
  Internal Antenna Gain (in5 dBm units)..... 11
  Diversity..... DIVERSITY_ENABLED
Performance Profile Parameters
  Configuration..... AUTOMATIC
  Interference threshold..... 10%
  Noise threshold..... -70 dBm
  RF utilization threshold..... 80%
  Data-rate threshold..... 1000000 bps
  Client threshold..... 12 clients
  Coverage SNR threshold..... 12 dB
  Coverage exception level..... 25%
  Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0
```

次に、Cisco アクセス ポイントの一般的な設定を表示する例を示します。

```
(Cisco Controller) >show ap config general cisco-ap
Cisco AP Identifier..... 9
Cisco AP Name..... cisco-ap
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A 802.11a:-A
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 1
MAC Address..... 12:12:12:12:12:12
IP Address Configuration..... DHCP
IP Address..... 10.10.10.21
IP NetMask..... 255.255.255.0
CAPWAP Path MTU..... 1485
Domain.....
```

```
Name Server.....................................
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ 4404
Primary Cisco Switch IP Address.................. 10.10.10.32
Secondary Cisco Switch Name.....................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name....................... 4404
Tertiary Cisco Switch IP Address................. 3.3.3.3
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Global: Disabled, Local: Disabled
AP subMode ...................................... WIPS
Remote AP Debug ................................. Disabled
S/W  Version .................................... 5.1.0.0
Boot  Version ................................... 12.4.10.0
Mini IOS Version ................................ 0.0.0.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Disabled
Power Type/Mode.................................. PoE/Low Power (degraded mode)
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1252AG-A-K9
IOS Version...................................... 12.4(10:0)
Reset Button..................................... Enabled
AP Serial Number................................. serial_number
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation........... Enabled (Global MFP Disabled)
AP User Mode..................................... CUSTOMIZED
AP username..................................... maria
AP Dot1x User Mode............................... Not Configured
AP Dot1x username................................ Not Configured
Cisco AP system logging host..................... 255.255.255.255
AP Up Time....................................... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time................................. 4 days, 06 h 15 m 00 s
Join Date and Time............................... Mon Mar 3 06:19:47 2008
Ethernet Port Duplex............................. Auto
Ethernet Port Speed.............................. Auto
AP Link Latency.................................. Enabled
 Current Delay................................... 0 ms
 Maximum Delay................................... 240 ms
 Minimum Delay................................... 0 ms
 Last updated (based on AP Up Time).............. 4 days, 06 h 17 m 20 s
Rogue Detection.................................. Enabled
AP TCP MSS Adjust................................ Disabled
Mesh preferred parent............................ 00:24:13:0f:92:00
```

show ap config general

すべてのアクセスポイントのアクセスポイント固有のsyslogサーバ設定を表示するには、**show ap config general** コマンドを使用します。

show ap config general

構文の説明

このコマンドには、引数およびキーワードはありません。

show ap config global

コントローラに結合されているアクセス ポイントすべてのグローバル syslog サーバ設定を表示するには、**show ap config global** コマンドを使用します。

show ap config global

構文の説明

このコマンドには、引数およびキーワードはありません。

次に、グローバル syslog サーバ設定を表示する例を示します。

```
(Cisco Controller) >show ap config global
AP global system logging host............................. 255.255.255.255
```

show ap core-dump

Lightweight アクセス ポイントのメモリ コア ダンプ情報を表示するには、 **show ap core-dump** コマンドを使用します。

show ap core-dump *cisco_ap*

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

次に、メモリ コア ダンプ情報を表示する例を示します。

```
(Cisco Controller) >show ap core-dump AP02
Memory core dump is disabled.
```

show ap crash-file

Lightweight アクセス ポイントによって生成されたクラッシュ ファイルおよび無線コア ダンプ ファイルの両方の一覧を表示するには、**show ap crash-file** コマンドを使用します。

show ap crash-file

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、アクセス ポイントで生成されたクラッシュ ファイルを表示する例を示します。

```
(Cisco Controller) >show ap crash-file
```

show ap data-plane

すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ プレーンのステータスを表示するには、**show ap data-plane** コマンドを使用します。

show ap data-plane {**all** | *cisco_ap* }

構文の説明

all	すべての Cisco Lightweight アクセス ポイントを指定します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

次に、すべてのアクセス ポイントのデータ プレーンのステータスを表示する例を示します。

```
(Cisco Controller) >show ap data-plane all
Min Data          Data          Max Data     Last
AP Name              Round Trip      Round Trip      Round Trip    Update
------------------  --------------  --------------  --------------  ------
1130                       0.000s          0.000s       0.002s     18:51:23
1240                       0.000s          0.000s       0.000s     18:50:45
```

show ap dtls-cipher-suite

DTLS show 暗号スイート情報を表示するには、**show ap dtls-cipher-suite** コマンドを使用します。

show ap dtls-cipher-suite

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、DTLS 暗号スイート情報を表示する例を示します。

```
(Cisco Controller) > show ap dtls-cipher-suite
DTLS Cipher Suite.............................. RSA-AES256-SHA
```

show ap ethernet tag

イーサネット インターフェイスの VLAN タギング情報を表示するには、**show ap ethernet tag** コマンドを使用します。

show ap ethernet tag {**summary** | *cisco_ap* }

構文の説明

summary	コントローラに関連付けられているすべてのアクセス ポイントの VLAN タギング情報を表示します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。コントローラに関連付けられている特定のアクセス ポイントの VLAN タギング情報を表示します。

コマンド デフォルト

なし

使用上のガイドライン

アクセス ポイントが指定したトランク VLAN を使用してトラフィックをルーティングできないか、コントローラに到達できない場合は、タグなし設定にフォールバックします。アクセス ポイントがこのフォール バック設定を使用してコントローラに接続すると、コントローラは WCS などのトラップ サーバにトランク VLAN の障害を示すトラップを送信します。このシナリオでは、show コマンドの出力に「Failover to untagged」というメッセージが表示されます。

次に、コントローラに関連付けられているすべてのアクセス ポイントの VLAN タギング情報を表示する例を示します。

```
(Cisco Controller) >show ap ethernet tag summary

AP Name              Vlan Tag Configuration
------------------   -------
AP2                  7  (Failover to untagged)
charan.AP1140.II     disabled
```

show ap eventlog

コントローラに結合されているアクセス ポイントのイベント ログ ファイルの内容を表示するには、**show ap eventlog** コマンドを使用します。

show ap eventlog *ap_name*

構文の説明

ap_name	指定したアクセス ポイントのイベント ログ。

コマンド デフォルト

なし

次に、アクセス ポイントのイベント ログを表示する例を示します。

```
(Cisco Controller) >show ap eventlog ciscoAP
AP event log download has been initiated
Waiting for download to complete
AP event log download completed.
======================= AP Event log Contents ====================
*Feb 13 11:54:17.146: %CAPWAP-3-CLIENTEVENTLOG: AP event log has been cleared from the
contoller 'admin'
*Feb 13 11:54:32.874: *** Access point reloading. Reason: Reload Command ***
*Mar 1 00:00:39.134: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:00:39.174: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Mar 1 00:00:39.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 00:00:49.947: %CAPWAP-3-CLIENTEVENTLOG: Did not get vendor specific options from
 DHCP.
...
```

show ap flexconnect

FlexConnect モードの AP の詳細を表示するには、**show ap flexconnect** コマンドを使用します。

show ap flexconnect module-vlan *ap-name*

構文の説明

module-vlan	FlexConnect ローカル スイッチングのステータスと VLAN ID 値を表示します。
ap-name	Cisco AP の名前。

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

show ap image

指定したアクセス ポイントについて事前にダウンロードされたイメージに関する詳細情報を表示するには、**show ap image** コマンドを使用します。

show ap image {*cisco_ap* | **all**}

構文の説明

cisco_ap	Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントを指定します。

（注） *all* という名前の AP があると、これはすべてのアクセス ポイントを指定するキーワード **all** と競合します。このシナリオでは、キーワード **all** が *all* という名前の AP よりも優先されます。

show ap inventory

アクセス ポイントのインベントリ情報を表示するには、**show ap inventory** コマンドを使用します。

show ap inventory {*ap-name* | **all**}

構文の説明

ap-name	指定された AP のインベントリ。
all	すべての AP のインベントリ。

コマンド デフォルト

なし

次に、アクセス ポイントのインベントリを表示する例を示します。

```
(Cisco Controller) >show ap inventory test101
NAME: "test101"    , DESCR: "Cisco Wireless Access Point"
PID: AIR-LAP1131AG-A-K9  ,  VID: V01,  SN: FTX1123T2XX
```

show ap join stats detailed

特定のアクセス ポイントについて収集された結合関連の統計をすべて表示するには、**show ap join stats detailed** コマンドを使用します。

show ap join stats detailed *ap_mac*

構文の説明

ap_mac	アクセス ポイント Ethernet MAC アドレス、または 802.11 無線インターフェイスの MAC アドレス。

コマンド デフォルト

なし

次に、コントローラを結合しようとする特定のアクセス ポイントの結合情報を表示する例を示します。

```
(Cisco Controller) >show ap join stats detailed 00:0b:85:02:0d:20
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23:335
- Time at last unsuccessful discovery attempt..... Not applicable
Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt.....RADIUS authorization is pending
 for the AP
- Time at last successful join attempt..... Aug 21 12:50:34:481
- Time at last unsuccessful join attempt..... Aug 21 12:50:34:374
Configuration phase statistics
- Configuration requests received..... 1
- Successful configuration responses sent..... 1
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt... Not applicable
- Time at last successful configuration attempt..... Aug 21 12:50:34:374
- Time at last unsuccessful configuration attempt..... Not applicable
Last AP message decryption failure details
- Reason for last message decryption failure..... Not applicable
Last AP disconnect details
- Reason for last AP connection failure..... Not applicable
Last join error summary
- Type of error that occurred last..... Lwapp join request rejected
- Reason for error that occurred last..... RADIUS authorization is pending
 for the AP
- Time at which the last join error occurred..... Aug 21 12:50:34:374
```

show ap join stats summary

特定のアクセス ポイントで最後に発生した結合エラーの詳細を表示するには、**show ap join stats summary** コマンドを使用します。

show ap join stats summary *ap_mac*

構文の説明

ap_mac	アクセス ポイント Ethernet MAC アドレス、または 802.11 無線インターフェイスの MAC アドレス。

コマンド デフォルト

なし

使用上のガイドライン

802.11 無線インターフェイスの MAC アドレスを取得するには、アクセス ポイントで **show interface** コマンドを入力します。

次に、アクセス ポイントの特定の結合情報を表示する例を示します。

```
(Cisco Controller) >show ap join stats summary 00:0b:85:02:0d:20
Is the AP currently connected to controller..... No
Time at which the AP joined this controller last time..... Aug 21 12:50:36:061
Type of error that occurred last..... Lwapp join request
 rejected
Reason for error that occurred last..... RADIUS authorization
 is pending for the AP
Time at which the last join error occurred..... Aug 21 12:50:34:374
```

show ap join stats summary all

コントローラに結合された、または結合が試行されたすべてのアクセス ポイントの MAC アドレスを表示するには、**show ap join stats summary all** コマンドを使用します。

show ap join stats summary all

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、すべてのアクセス ポイントの結合情報のサマリーを表示する例を示します。

```
(Cisco Controller) >show ap join stats summary all
Number of APs.......................................... 4
Base Mac             AP EthernetMac         AP Name          IP Address         Status
00:0b:85:57:bc:c0     00:0b:85:57:bc:c0     AP1130          10.10.163.217     Joined
00:1c:0f:81:db:80     00:1c:63:23:ac:a0     AP1140          10.10.163.216     Not joined
00:1c:0f:81:fc:20     00:1b:d5:9f:7d:b2     AP1              10.10.163.215     Joined
00:21:1b:ea:36:60     00:0c:d4:8a:6b:c1     AP2             10.10.163.214     Not joined
```

show ap led-state

すべてのアクセス ポイントまたは特定のアクセス ポイントの LED の状態を表示するには、**show ap led-state** コマンドを使用します。

show ap led-state {**all** | *cisco_ap* }

構文の説明

all	すべてのアクセスポイントのLEDの状態を示します。
cisco_ap	LED の状態を示すアクセス ポイントの名前。

コマンド デフォルト

AP の LED 状態が有効です。

次に、すべてのアクセス ポイントの LED の状態を取得する例を示します。

```
(Cisco Controller) >show ap led-state all
Global LED State: Enabled (default)
```

show ap led-flash

アクセス ポイントの LED のフラッシュ ステータスを表示するには、**show ap led-flash** コマンドを使用します。

show ap led-flash *cisco_ap*

構文の説明

cisco_ap	Cisco AP の名前を入力します。

コマンド デフォルト

なし

次に、アクセス ポイントの LED フラッシュ ステータスを表示する例を示します。

```
(Cisco Controller) >show ap led-flash
```

show ap link-encryption

コントローラに結合された、または結合が試行されたすべてのアクセス ポイントの MAC アドレスを表示するには、**show ap link-encryption** コマンドを使用します。

show ap link-encryption {**all** | *cisco_ap* }

構文の説明

all	すべてのアクセス ポイントを指定します。
cisco_ap	Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのアクセス ポイントのリンク暗号化ステータスを表示する例を示します。

```
(Cisco Controller) >show ap link-encryption all
             Encryption  Dnstream  Upstream    Last
AP Name           State     Count     Count  Update
------------------  ---  --------  --------  ------
1240                Dis       4406    237553   Never
1130                 En       2484    276308   19:31
```

show ap max-count summary

Cisco WLC でサポートされるアクセス ポイントの最大数を表示するには、**show ap max-count summary** コマンドを使用します。

show ap max-count summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、**show ap max-count summary** コマンドの出力例を示します。

```
(Cisco Controller) >show ap max-count

The max number of AP's supported.................. 500
```

show ap monitor-mode summary

チャネルに最適化された監視モードの現在の設定を表示するには、**show ap monitor-mode summary** コマンドを使用します。

show ap monitor-mode summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、チャネルに最適化された監視モードの現在の設定を表示する例を示します。

```
(Cisco Controller) >show ap monitor-mode summary
AP Name            Ethernet MAC       Status     Scanning Channel List
---  ----------------  ----------  ----------------------
AP_004             xx:xx:xx:xx:xx:xx Tracking    1, 6, 11, 4
```

show ap module summary

特定の Cisco AP またはすべての Cisco AP の外部モジュールについての詳細情報を表示するには、**show ap module summary** コマンドを使用します。

show ap module summary {*ap-name* | **all**}

構文の説明

ap-name	外部モジュールを持つ Cisco AP 名
all	外部モジュールを持つすべての Cisco AP

show ap packet-dump status

アクセス ポイントのパケット キャプチャ設定を表示するには、**show ap packet-dump status** コマンドを使用します。

show ap packet-dump status

構文の説明

このコマンドには引数またはキーワードはありません。

使用上のガイドライン

コントローラ間ローミング中には、パケット キャプチャは機能しません。

コントローラでは、ビーコンやプローブの応答などの、無線ファームウェアに作成され、アクセス ポイントから送信されたパケットをキャプチャしません。Tx パスで無線ドライバから伝送されるパケットだけがキャプチャされます。

次に、アクセス ポイントのパケット キャプチャ設定を表示する例を示します。

```
(Cisco Controller) >show ap packet-dump status
Packet Capture Status..................................... Stopped
FTP Server IP Address..................................... 0.0.0.0
FTP Server Path...........................................
FTP Server Username.......................................
FTP Server Password....................................... ********
Buffer Size for Capture................................... 2048 KB
Packet Capture Time....................................... 45 Minutes
Packet Truncate Length.................................... Unspecified
Packet Capture Classifier................................. None
```

show ap prefer-mode stats

グローバル優先モードおよびAPグループごとの統計情報を表示するには、**show ap prefer-mode stats** コマンドを使用します。

show ap prefer-mode stats

構文の説明

stats	グローバル優先モードおよびAPグループごとの統計情報を表示します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

show ap retransmit

アクセス ポイントの制御パケット再送信パラメータを表示するには、**show ap retransmit** コマンドを使用します。

show ap retransmit {**all** | *cisco_ap* }

構文の説明

all	すべてのアクセス ポイントを指定します。
cisco_ap	アクセス ポイントの名前。

コマンド デフォルト

なし

次に、ネットワーク上のすべてのアクセス ポイントの制御パケット再送信パラメータを表示する例を示します。

```
(Cisco Controller) >show ap retransmit all
Global control packet retransmit interval: 3 (default)
Global control packet retransmit count: 5 (default)
AP Name             Retransmit Interval  Retransmit count
------------------  -------------------  -------------------
AP_004                   3 (default)      5 (WLC default),5 (AP default)
```

show ap stats

Cisco Lightweight アクセス ポイントの統計情報を表示するには、**show ap stats** コマンドを使用します。

show ap stats {**802.11**{**a** | **b**} | **wlan** | **ethernet summary**} *cisco_ap* [**tsm** {*client_mac* | **all**}]

構文の説明

802.11a	802.11a ネットワークを指定します
802.11b	802.11b/g ネットワークを指定します。
wlan	WLAN 統計情報を指定します。
ethernet	APイーサネットインターフェイス統計情報を指定します。
summary	接続されたすべての Cisco アクセス ポイントのイーサネット インターフェイスの要約を表示します。
cisco_ap	Lightweight アクセス ポイントの名前。
tsm	（任意）トラフィック ストリーム メトリックを指定します。
client_mac	（任意）選択クライアントのMACアドレス。
all	（任意）すべてのアクセス ポイントを指定します。

コマンド デフォルト

なし

次に、802.11bネットワークのアクセスポイントの統計情報を表示する例を示します。

```
(Cisco Controller) >show ap stats 802.11a Ibiza

Number Of Slots.................................. 2
AP Name.......................................... Ibiza
MAC Address...................................... 44:2b:03:9a:8a:73
Radio Type....................................... RADIO_TYPE_80211a
Stats Information
  Number of Users................................ 0
  TxFragmentCount................................ 84628
  MulticastTxFrameCnt............................ 84628
  FailedCount.................................... 0
  RetryCount..................................... 0
  MultipleRetryCount............................. 0
  FrameDuplicateCount............................ 0
  RtsSuccessCount................................ 1
  RtsFailureCount................................ 0
```

```
  AckFailureCount.............................. 0
  RxIncompleteFragment......................... 0
  MulticastRxFrameCnt.......................... 0
  FcsErrorCount................................ 20348857
  TxFrameCount................................. 84628
  WepUndecryptableCount........................ 19907
  TxFramesDropped.............................. 0
OEAP WMM Stats :
  Best Effort:
    Tx Frame Count............................. 0
    Tx Failed Frame Count...................... 0
    Tx Expired Count........................... 0
    Tx Overflow Count.......................... 0
    Tx Queue Count............................. 0
    Tx Queue Max Count......................... 0
    Rx Frame Count............................. 0
    Rx Failed Frame Count...................... 0
  Background:
    Tx Frame Count............................. 0
    Tx Failed Frame Count...................... 0
    Tx Expired Count........................... 0
    Tx Overflow Count.......................... 0
    Tx Queue Count............................. 0
    Tx Queue Max Count......................... 0
    Rx Frame Count............................. 0
    Rx Failed Frame Count...................... 0
  Video:
    Tx Frame Count............................. 0
    Tx Failed Frame Count...................... 0
    Tx Expired Count........................... 0
    Tx Overflow Count.......................... 0
    Tx Queue Count............................. 0
    Tx Queue Max Count......................... 0
    Rx Frame Count............................. 0
    Rx Failed Frame Count...................... 0
  Voice:
    Tx Frame Count............................. 0
    Tx Failed Frame Count...................... 0
    Tx Expired Count........................... 0
    Tx Overflow Count.......................... 0
    Tx Queue Count............................. 0
    Tx Queue Max Count......................... 0
    Rx Frame Count............................. 0
    Rx Failed Frame Count...................... 0

Rate Limiting Stats:
  Wlan 1:
    Number of Data Packets Received.............. 592
    Number of Data Rx Packets Dropped............ 160
    Number of Data Bytes Received................ 160783
    Number of Data Rx Bytes Dropped.............. 0
    Number of Realtime Packets Received.......... 592
    Number of Realtime Rx Packets Dropped........ 0
    Number of Realtime Bytes Received............ 160783
    Number of Realtime Rx Bytes Dropped.......... 0
    Number of Data Packets Sent.................. 131
    Number of Data Tx Packets Dropped............ 0
    Number of Data Bytes Sent.................... 23436
    Number of Data Tx Bytes Dropped.............. 0
    Number of Realtime Packets Sent.............. 131
    Number of Realtime Tx Packets Dropped........ 0
    Number of Realtime Bytes Sent................ 23436
    Number of Realtime Tx Bytes Dropped.......... 0
Call Admission Control (CAC) Stats
```

```
  Voice Bandwidth in use(% of config bw)..... 0
  Voice Roam Bandwidth in use(% of config bw).... 0
    Total channel MT free..................... 0
    Total voice MT free....................... 0
    Na Direct................................. 0
    Na Roam................................... 0
  Video Bandwidth in use(% of config bw)..... 0
  Video Roam Bandwidth in use(% of config bw).... 0
  Total BW in use for Voice(%)............... 0
  Total BW in use for SIP Preferred call(%)...... 0
WMM TSPEC CAC Call Stats
  Total num of voice calls in progress.......... 0
  Num of roaming voice calls in progress........ 0
  Total Num of voice calls since AP joined...... 0
  Total Num of roaming calls since AP joined..... 0
  Total Num of exp bw requests received......... 0
  Total Num of exp bw requests admitted......... 0
  Num of voice calls rejected since AP joined.... 0
  Num of roam calls rejected since AP joined..... 0
  Num of calls rejected due to insufficent bw.... 0
  Num of calls rejected due to invalid params.... 0
  Num of calls rejected due to PHY rate......... 0
  Num of calls rejected due to QoS policy........ 0
SIP CAC Call Stats
  Total Num of calls in progress................ 0
  Num of roaming calls in progress.............. 0
  Total Num of calls since AP joined............ 0
  Total Num of roaming calls since AP joined..... 0
  Total Num of Preferred calls received......... 0
  Total Num of Preferred calls accepted......... 0
  Total Num of ongoing Preferred calls.......... 0
  Total Num of calls rejected(Insuff BW)........ 0
  Total Num of roam calls rejected(Insuff BW).... 0
WMM Video TSPEC CAC Call Stats
  Total num of video calls in progress.......... 0
  Num of roaming video calls in progress........ 0
  Total Num of video calls since AP joined...... 0
  Total Num of video roaming calls since AP j.... 0
  Num of video calls rejected since AP joined.... 0
  Num of video roam calls rejected since AP j.... 0
  Num of video calls rejected due to insuffic.... 0
  Num of video calls rejected due to invalid .... 0
  Num of video calls rejected due to PHY rate.... 0
  Num of video calls rejected due to QoS poli.... 0
SIP Video CAC Call Stats
  Total Num of video calls in progress.......... 0
  Num of video roaming calls in progress........ 0
  Total Num of video calls since AP joined...... 0
  Total Num of video roaming calls since AP j.... 0
  Total Num of video calls rejected(Insuff BW.... 0
  Total Num of video roam calls rejected(Insu.... 0
Band Select Stats
  Num of dual band client ...................... 0
  Num of dual band client added................. 0
  Num of dual band client expired .............. 0
  Num of dual band client replaced.............. 0
  Num of dual band client detected ............. 0
  Num of suppressed client ..................... 0
  Num of suppressed client expired.............. 0
  Num of suppressed client replaced............. 0
```

show ap summary

コントローラに接続されているすべてのLightweightアクセス ポイントの要約を表示するには、**show ap summary** コマンドを使用します。

show ap summary [*cisco_ap*]

構文の説明

cisco_ap	（任意）特定のAPの名前またはAPのグループを構成する文字のシーケンスを入力するか、ワイルド文字検索パターンを入力します。

コマンド デフォルト

なし

使用上のガイドライン

各Lightweightアクセス ポイント名、スロット数、製造元、MACアドレス、ロケーション、コントローラのポート番号が含まれるリストが表示されます。指定しました。

次に、接続されているすべてのアクセス ポイントの要約を表示する例を示します。

```
(Cisco Controller) >show ap summary
Number of APs.................................... 2
Global AP username............................... user
Global AP Dot1x username......................... Not Configured
Number of APs.................................... 2
Global AP username............................... user
Global AP Dot1x username......................... Not Configured


 AP Name             Slots  AP Model              Ethernet MAC       Location
Country  IP Address       Clients
------------------  -----  --------------------  -----------------  -----------------
-------  ---------------  -------
AP1140              2     AIR-LAP1142N-A-K9     f0:f7:55:75:f3:29               default
 location         US   192.168.0.0         0
Access Points using IPv6 transport:
 AP Name    Slots   AP Model           Ethernet MAC       Location         Country
IPv6 Address                Clients
 ------------------ ----- ------------------------------------ ------------
------------------ ----- ---------------------------- ------
 AP1040      2    AIR-LAP1042N-A-K9   00:40:96:b9:4b:89   default location  US
2001:DB8:0:1::1                     0
```

show ap tcp-mss-adjust

アクセス ポイントに定義されている各 WLAN の Basic Service Set Identifier（BSSID）値を表示するには、**show ap tcp-mss-adjust** コマンドを使用します。

show ap tcp-mss-adjust {*cisco_ap* | **all**}

構文の説明

cisco_ap	指定した Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントを指定します。

（注） AP 自体が **all** キーワードで設定されている場合、all access points の場合は **all** というキーワードを持つ AP に優先します。

次に、すべてのアクセス ポイントの Transmission Control Protocol（TCP）の最大セグメント サイズ（MSS）の情報を表示する例を示します。

```
(Cisco Controller) >show ap tcp-mss-adjust all
AP Name            TCP State MSS Size
------------------ --------- -------
AP-1140            enabled   536
AP-1240            disabled  -
AP-1130            disabled  -
```

show ap wlan

アクセス ポイントに定義されている各 WLAN の Basic Service Set Identifier（BSSID）値を表示するには、**show ap wlan** コマンドを使用します。

show ap wlan 802.11{**a** | **b**} *cisco_ap*

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b/g ネットワークを指定します。
ap_name	Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

次に、802.11b ネットワークのアクセス ポイントの BSSID を表示する例を示します。

```
(Cisco Controller) >show ap wlan 802.11b AP01
Site Name..................................... MY_AP_GROUP1
Site Description.............................. MY_AP_GROUP1
WLAN ID          Interface          BSSID
-------         -----------        -------------------------
1               management           00:1c:0f:81:fc:20
2               dynamic              00:1c:0f:81:fc:21
```

show assisted-roaming

経由ローミングと 802.11k 設定を表示するには、**show assisted-roaming** コマンドを使用します。

show assisted-roaming

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、経由ローミングと 802.11k 設定を表示する例を示します。

```
(Cisco Controller) >show assisted-roaming
Assisted Roaming and 80211k Information:
Floor RSSI Bias.............................. 15 dBm
Maximum Denial............................... 2 counts
Minimium Optimized Neighbor Assigned............. 2 neighbors

Assisted Roaming Performance Chart:
Matching Assigned Neighbor..................... [0] = 0
Matching Assigned Neighbor..................... [1] = 0
Matching Assigned Neighbor..................... [2] = 0
Matching Assigned Neighbor..................... [3] = 0
Matching Assigned Neighbor..................... [4] = 0
Matching Assigned Neighbor..................... [5] = 0
Matching Assigned Neighbor..................... [6] = 0
Matching Assigned Neighbor..................... [7] = 0
No Matching Neighbor........................... [8] = 0
No Neighbor Assigned........................... [9] = 0
```

関連コマンド

config assisted-roaming

config wlan assisted-roaming

debug 11k

show atf config

Cisco Air Time Fairness の設定を監視するには、**show atf config** コマンドを使用します。

show atf config {**all** | {**ap-name***ap-name*} | {**802.11**{**a** | **b**}} | **policy** | **wlan**}

構文の説明

all	すべての無線の Cisco ATF 設定を表示します。
ap-name	AP の Cisco ATF 設定を表示します。
ap-name	指定する必要がある AP 名。
802.11a	すべての 5-GHz 無線の Cisco ATF 設定を表示します。
802.11b	すべての 2.4-GHz 無線の Cisco ATF 設定を表示します。
policy	すべての通信時間ポリシーの設定を表示します。
wlan	すべての WLAN の Cisco ATF 設定を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが追加されました。

次に、Cisco Airtime Fairness の設定を監視する例を示します。

```
(Cisco Controller) >show atf config all
```

show atf statistics ap

Cisco Air Time Fairness の統計情報を監視するには、**show atf statistics** コマンドを使用します。

show atf statistics ap *ap-name* **802.11**{**a** | **b**} {**summary** | *wlan-id* | *policy-id*}

構文の説明

802.11a	すべての 5-GHz 無線の詳細な統計情報を表示します。
802.11b	すべての 2.4-GHz 無線の詳細な統計情報を表示します。
summary	AP の統計情報の要約を表示します。
wlan *wlan-id*	指定した WLAN の詳細な ATF 統計情報を表示します。
policy *policy-name*	指定したポリシー名の詳細な ATF 統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、Cisco Airtime Fairness の統計情報を監視する例を示します。

```
(Cisco Controller) >show atf statistics ap Ap01323 802.11a summary
```

show auth-list

アクセス ポイントの認証リストを表示するには、**show auth-list** コマンドを使用します。

show auth-list

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントの認証リストを表示する例を示します。

```
(Cisco Controller) >show auth-list
Authorize APs against AAA..................... disabled
Allow APs with Self-signed Certificate (SSC)... disabled
Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ----------------------------------------
xx:xx:xx:xx:xx:xx         MIC
```

show avc applications

すべてのサポートされる Application Visibility and Control（AVC）アプリケーションを表示するには、**show avc applications** コマンドを使用します。

show avc applications

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

使用上のガイドライン

AVC は、Network-Based Application Recognition（NBAR）ディープ パケット インスペクション テクノロジーを使用し、アプリケーションが使用するプロトコルに基づいてアプリケーションを分類します。AVC を使用して、コントローラは 1500 を超えるレイヤ 4 からレイヤ 7 へのプロトコルを検出できます。

次に、**show avc applications** コマンドの出力例を示します。

```
(Cisco Controller) > show avc applications

Application-Name            App-ID  Engine-ID  Selector-ID   Application-Group-Name
 ================            ======  =========  ===========   ======================
 3com-amp3                     538         3        629        other
 3com-tsmux                    977         3        106        obsolete
 3pc                           788         1         34        layer3-over-ip
 914c/g                       1109         3        211        net-admin
 9pfs                          479         3        564        net-admin
 acap                          582         3        674        net-admin
 acas                          939         3         62        other
 accessbuilder                 662         3        888        other
 accessnetwork                 607         3        699        other
 acp                           513         3        599        other
 acr-nema                      975         3        104        industrial-protocols
 active-directory             1194        13        473        other
 activesync                   1419      13       490        business-and-productivity-tools

 adobe-connect                1441       13       505        other
 aed-512                       963        3       149        obsolete
 afpovertcp                   1327       3       548        business-and-productivity-tools

 agentx                        609         3        705        net-admin
 alpes                         377         3        463        net-admin
 aminet                        558         3       2639        file-sharing
 an                            861         1        107        layer3-over-ip
----                           ----       ---      -----       -------------
```

show avc engine

Network-Based Application Recognition 2（NBAR2）エンジンに関する情報を表示するには、**show avc engine** コマンドを使用します。

show avc engine version

構文の説明

version	NBAR2 エンジンのバージョンを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

Application Visibility and Control（AVC）プロトコル パックは、Cisco 2500 シリーズ ワイヤレス コントローラではサポートされていません。

次に、**show avc engine** コマンドの出力例を示します。

```
(Cisco Controller) > show avc engine version

AVC Engine Version: 13
```

show avc profile

Application Visibility and Control（AVC）プロファイルを表示するには、**show avc profile** コマンドを使用します。

show avc profile {**summary** | **detailed** *profile_name* }

構文の説明

summary	AVC プロファイルの要約を表示します。
detailed	AVC プロファイルの詳細を表示します。
profile_name	AVC プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、**show avc profile summary** コマンドの出力例を示します。

```
(Cisco Controller) > show avc profile summary

 Profile-Name                      Number of Rules
  ============                      ==============
  profile 1                                3
  avc_profile2                             1
```

次に、**show avc profile detailed** コマンドの出力例を示します。

```
(Cisco Controller) > show avc profile detailed

  Application-Name          Application-Group-Name            Action  DSCP
  ================          ======================            ======  ====
  ftp                       file-sharing                       Drop      -
  flash-video               browsing                           Mark     10
  facebook                  browsing                           Mark     10

  Associated WLAN IDs       :
  Associated Remote LAN IDs :
  Associated Guest LAN IDs  :
```

show avc protocol-pack

Cisco Wireless LAN Controller（WLC）の Application Visibility and Control（AVC）プロトコル パックについての情報を表示するには、**show avc protocol-pack** コマンドを使用します。

show avc protocol-pack version

構文の説明

version	AVC プロトコル パックのバージョンを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

AVC プロトコル パックは Cisco 2500 シリーズ ワイヤレス コントローラではサポートされていません。

次に、**show avc protocol-pack** コマンドの出力例を示します。

```
(Cisco Controller) > show avc protocol-pack version

AVC Protocol Pack Name: Advanced Protocol Pack
AVC Protocol Pack Version: 1.0
```

show avc statistics application

アプリケーションの統計情報を表示するには、**show avc statistics application** コマンドを使用します。

show avc statistics application *application_name* **top-users**［**downstream wlan** | **upstream wlan** | **wlan**］［*wlan_id* ］}

構文の説明

application_name	アプリケーションの名前。ライセンス名は最大 32 文字の英数字で、大文字と小文字を区別します。
top-users	上位のアプリケーション ユーザの AVC 統計情報を表示します。
downstream	（任意）上位のダウンストリーム アプリケーションの統計情報を表示します。
wlan	（任意）WLAN の AVC 統計情報を表示します。
wlan_id	1～512 の WLAN 識別子。
upstream	（任意）上位のアップストリーム アプリケーションの統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、**show avc statistics application** コマンドの出力例を示します。

```
(Cisco Controller) > show avc statistics application ftp top-users downstream wlan 1

 Client MAC            Client IP        WLAN ID  Packets   Bytes   Avg Pkt  Packets
Bytes       DSCP
 (Up/Down)                                       (n secs) (n secs)  Size    (Total)
(Total)   In  Out
 ============          =========        ======   =======  =======  ======   =======
=======   === ===
 00:0a:ab:15:00:9c(U) 172.16.31.156        1         16        91     5         43
    338     0   0
                  (D) 172.16.31.156        1         22      5911   268         48
   6409     0   0
 00:0a:ab:15:00:5a(U) 172.16.31.90         1          7        39     5         13
     84     0   0
                  (D) 172.16.31.90         1         12      5723   476         18
   5869     0   0
 00:0a:ab:15:00:60(U) 172.16.31.96         1         19       117     6         75
   8666     0   0
                  (D) 172.16.31.96         1         19      4433   233         83
   9595     0   0
```

```
00:0a:ab:15:00:a4(U) 172.16.31.164        1         18       139     7          21
   161     0   0
                (D) 172.16.31.164        1         23      4409   191          24
  4439     0   0
00:0a:ab:15:00:48(U) 172.16.31.72         1         21      2738   130          21
  2738     0   0
                (D) 172.16.31.72         1         22      4367   198          22
  4367     0   0
00:0a:ab:15:00:87(U) 172.16.31.135        1         11        47     4          49
   301     0   0
                (D) 172.16.31.135        1         12      4208   350          48
  7755     0   0
00:0a:ab:15:00:92(U) 172.16.31.146        1         10        73     7          11
    84     0   0
                (D) 172.16.31.146        1          9      4168   463          11
  4201     0   0
00:0a:ab:15:00:31(U) 172.16.31.49         1         11        95     8          34
   250     0   0
                (D) 172.16.31.49         1         18      3201   177          43
  3755     0   0
00:0a:ab:15:00:46(U) 172.16.31.70         1          7        47     6          20
   175     0   0
                (D) 172.16.31.70         1         10      3162   316          23
  3448     0   0
00:0a:ab:15:00:b3(U) 172.16.31.179        1         10        85     8          34
   241     0   0
```

show avc statistics client

クライアントの Application Visibility and Control（AVC）統計情報を表示するには、**show avc statistics client** コマンドを使用します。

show avc statistics client *client_MAC* {**application** *application_name* | **top-apps** [**upstream** | **downstream**]}

構文の説明

client_MAC	クライアントの MAC アドレス。
application	アプリケーションの AVC 統計情報を表示します。
application_name	アプリケーションの名前。ライセンス名は最大32文字の英数字で、大文字と小文字を区別します。
top-apps	上位のアプリケーションの AVC 統計情報を表示します。
upstream	（任意）上位のアップストリームアプリケーションの統計情報を表示します。
downstream	（任意）上位のダウンストリームアプリケーションの統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、**show avc statistics client** コマンドの出力例を示します。

```
(Cisco Controller) > show avc statistics client 00:0a:ab:15:00:01 application http

 Description                   Upstream      Downstream
  ===========                   ========      ==========
  Number of Packtes(n secs)         5059            6369
  Number of Bytes(n secs)         170144         8655115
  Average Packet size(n secs)         33            1358
  Total Number of Packtes         131878          150169
  Total Number of Bytes          6054464       205239972
  DSCP Incoming packet                16               0
  DSCP Outgoing Packet                16               0
```

次に、**show avc statistics client** コマンドの出力例を示します。

```
(Cisco Controller) > show avc statistics client 00:0a:ab:15:00:01 top-apps

  Application-Name           Packets   Bytes    Avg Pkt  Packets    Bytes    DSCP DSCP
      (Up/Down)              (n secs)  (n secs)  Size    (Total)   (Total)    In   Out
  ================           =======   ======   ======   =======   ======    ====  ====
```

http	(U)	6035	637728	105	6035	637728	16	16
	(D)	5420	7218796	1331	5420	7218796	0	0
ggp	(U)	1331	1362944	1024	1331	1362944	0	0
	(D)	0	0	0	0	0	0	0
smp	(U)	1046	1071104	1024	1046	1071104	0	0
	(D)	0	0	0	0	0	0	0
vrrp	(U)	205	209920	1024	205	209920	0	0
	(D)	0	0	0	0	0	0	0
bittorrent	(U)	117	1604	13	117	1604	0	0
	(D)	121	70469	582	121	70469	0	0
icmp	(U)	0	0	0	0	0	0	0
	(D)	72	40032	556	72	40032	48	48
edonkey	(U)	112	4620	41	112	4620	0	0
	(D)	105	33076	315	105	33076	0	0
dns	(U)	10	380	38	10	380	0	0
	(D)	7	1743	249	7	1743	0	0
realmedia	(U)	2	158	79	2	158	24	24
	(D)	2	65	32	2	65	0	0

show avc statistics guest-lan

ゲスト LAN の Application Visibility and Control（AVC）統計情報を表示するには、**show avc statistics guest-lan** コマンドを使用します。

show avc statistics guest-lan *guest-lan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

構文の説明

guest-lan_id	1 ～ 5 のゲスト LAN 識別子
application	アプリケーションの AVC 統計情報を表示します。
application_name	アプリケーションの名前。ライセンス名は最大 32 文字の英数字で、大文字と小文字を区別します。
top-app-groups	上位のアプリケーション グループの AVC 統計情報を表示します。
upstream	（任意）上位のアップストリーム アプリケーションの統計情報を表示します。
downstream	（任意）上位のダウンストリーム アプリケーションの統計情報を表示します。
top-apps	上位のアプリケーションの AVC 統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、**show avc statistics** コマンドの出力例を示します。

```
(Cisco Controller) > show avc statistics guest-lan 1

Application-Name              Packets   Bytes   Avg Pkt  Packets      Bytes
  (Up/Down)                   (n secs) (n secs)  Size    (Total)      (Total)
================              =======  ======    ======   ======      =======
unclassified             (U)  191464    208627     1    92208613  11138796586
                         (D)  63427  53440610   842    16295621   9657054635
ftp                      (U)    805     72880    90      172939     11206202
                         (D)    911     58143    63      190900     17418653
http                     (U)  264904  12508288    47    27493945   2837672192
                         (D)  319894  436915253  1365    29850934  36817587924
gre                      (U)      0         0     0    10158872  10402684928
                         (D)      0         0     0           0            0
icmp                     (U)      1        40    40         323        98476
                         (D)   7262   4034576   555     2888266   1605133372
ipinip                   (U)  62565  64066560  1024    11992305  12280120320
                         (D)      0         0     0           0            0
```

imap	(U)	1430	16798	11	305161	3795766
	(D)	1555	576371	370	332290	125799465
irc	(U)	9	74	8	1736	9133
	(D)	11	371	33	1972	173381
nntp	(U)	22	158	7	1705	9612
	(D)	22	372	16	2047	214391

show avc statistics remote-lan

リモート LAN の Application Visibility and Control（AVC）統計情報を表示するには、**show avc statistics remote-lan** コマンドを使用します。

show avc statistics remote-lan *remote-lan_id*{**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

構文の説明

remote-lan_id	1～512 のリモート LAN 識別子。
application	アプリケーションの AVC 統計情報を表示します。
application_name	アプリケーションの名前。ライセンス名は最大 32 文字の英数字で、大文字と小文字を区別します。
top-app-groups	上位のアプリケーション グループの AVC 統計情報を表示します。
upstream	（任意）上位のアップストリーム アプリケーションの統計情報を表示します。
downstream	（任意）上位のダウンストリーム アプリケーションの統計情報を表示します。
top-apps	上位のアプリケーションの AVC 統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、**show avc statistics remote-lan** コマンドの出力例を示します。

```
(Cisco Controller) > show avc statistics remote-lan 1

Application-Name              Packets   Bytes   Avg Pkt  Packets      Bytes
  (Up/Down)                   (n secs) (n secs)  Size    (Total)      (Total)
================              =======  ======    ======   ======      =======
unclassified            (U)  191464    208627     1    92208613  11138796586
                        (D)  63427  53440610   842    16295621   9657054635
ftp                     (U)    805     72880    90      172939     11206202
                        (D)    911     58143    63      190900     17418653
http                    (U)  264904  12508288    47    27493945   2837672192
                        (D)  319894  436915253  1365    29850934  36817587924
gre                     (U)      0         0     0    10158872  10402684928
                        (D)      0         0     0           0            0
icmp                    (U)      1        40    40         323        98476
                        (D)   7262   4034576   555     2888266   1605133372
ipinip                  (U)  62565  64066560  1024    11992305  12280120320
                        (D)      0         0     0           0            0
```

```
imap                    (U)   1430     16798    11       305161      3795766
                        (D)   1555    576371   370       332290    125799465
irc                     (U)      9        74     8         1736         9133
                        (D)     11       371    33         1972       173381
nntp                    (U)     22       158     7         1705         9612
                        (D)     22       372    16         2047       214391
```

show avc statistics top-apps

最も使用されているアプリケーションの Application Visibility and Control（AVC）統計情報を表示するには、**show avc statistics top-apps** コマンドを使用します。

show avc statistics top-apps［**upstream** | **downstream**］

構文の説明

upstream	（任意）最も使用されているアップストリームアプリケーションの統計情報を表示します。
downstream	（任意）最も使用されているダウンストリームアプリケーションの統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、**show avc statistics top-apps** コマンドの出力例を示します。

```
(Cisco Controller) > show avc statistics top-apps

Application-Name              Packets     Bytes   Avg Pkt     Packets         Bytes
   (Up/Down)                  (n secs)   (n secs)  Size       (Total)        (Total)
================              =======    =======  =======     =======        ========
http                    (U)    204570   10610912     51      28272539      2882294016
                        (D)    240936  327624221   1359      30750570     38026889010
realmedia               (U)       908      62154     68        400698        26470359
                        (D)    166694  220522943   1322      35802836     47131836785
mpls-in-ip              (U)     77448   79306752   1024      10292787     10539813888
                        (D)         0          0      0             0             0
fire                    (U)     70890   72591360   1024      10242484     10488303616
                        (D)         0          0      0             0             0
pipe                    (U)     68296   69935104   1024      10224255     10469637120
                        (D)         0          0      0             0             0
gre                     (U)     60982   62445568   1024      10340221     10588386304
                        (D)         0          0      0             0             0
crudp                   (U)     26430   27064320   1024      10109812     10352447488
                        (D)         0          0      0             0             0
rtp                     (U)         0          0      0             0             0
                        (D)      7482    9936096   1328       2603923      3458009744
icmp                    (U)         0          0      0           323           98476
                        (D)     10155    5640504    555       2924693      1625363564
```

関連コマンド

config avc profile delete

config avc profile create

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics client

show avc statistics wlan

show avc statistics applications

show avc statistics guest-lan

show avc statistics remote-lan

debug avc error

debug avc events

show avc statistics wlan

WLAN の Application Visibility and Control（AVC）統計情報を表示するには、**show avc statistics wlan** コマンドを使用します。

show avc statistics wlan *wlan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

構文の説明

wlan_id	1～512 の WLAN 識別子。
application	アプリケーションの AVC 統計情報を表示します。
application_name	アプリケーションの名前。ライセンス名は最大 32 文字の英数字で、大文字と小文字を区別します。
top-app-groups	上位のアプリケーション グループの AVC 統計情報を表示します。
upstream	（任意）上位のアップストリーム アプリケーションの統計情報を表示します。
downstream	（任意）上位のダウンストリーム アプリケーションの統計情報を表示します。
top-apps	上位のアプリケーションの AVC 統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、**show avc statistics** コマンドの出力例を示します。

```
(Cisco Controller) >show avc statistics wlan 1

Application-Name              Packets   Bytes   Avg Pkt  Packets      Bytes
  (Up/Down)                   (n secs) (n secs)  Size    (Total)      (Total)
================              =======  ======    ======   ======      =======
unclassified             (U)  191464    208627     1    92208613  11138796586
                         (D)  63427  53440610   842    16295621   9657054635
ftp                      (U)    805     72880    90      172939     11206202
                         (D)    911     58143    63      190900     17418653
http                     (U)  264904  12508288    47    27493945   2837672192
                         (D)  319894  436915253  1365    29850934  36817587924
gre                      (U)      0         0     0    10158872  10402684928
                         (D)      0         0     0           0            0
icmp                     (U)      1        40    40         323        98476
                         (D)   7262   4034576   555     2888266   1605133372
ipinip                   (U)  62565  64066560  1024    11992305  12280120320
                         (D)      0         0     0           0            0
```

```
imap                    (U)    1430     16798     11       305161      3795766
                        (D)    1555    576371    370       332290    125799465
irc                     (U)       9        74      8         1736         9133
                        (D)      11       371     33         1972       173381
nntp                    (U)      22       158      7         1705         9612
                        (D)      22       372     16         2047       214391
```

次に、**show avc statistics wlan** コマンドの出力例を示します。

```
(Cisco Controller) >show avc statistics wlan 1 application ftp

Description                    Upstream    Downstream
 ===========                    ========    ==========
 Number of Packtes(n secs)             0             0
 Number of Bytes(n secs)               0             0
 Average Packet size(n secs)           0             0
 Total Number of Packtes           32459         64888
 Total Number of Bytes               274      94673983
```

show boot

プライマリおよびバックアップ ソフトウェアのビルド番号、またどちらのソフトウェアがアクティブかを表示するには、**show boot** コマンドを使用します。

show boot

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

各 Cisco ワイヤレス LAN コントローラは、プライマリとバックアップのオペレーティング システム ソフトウェア ロードをそれぞれ 1 つずつ不揮発性 RAM に保持することで、コントローラが必要に応じてプライマリ ロードをブートオフしたり（デフォルト）、バックアップ ロードに戻ったりできるようにします。

次に、**show boot** コマンドの出力例を示します。

```
(Cisco Controller) > show boot
Primary Boot Image.............................. 3.2.13.0 (active)
Backup Boot Image............................... 3.2.15.0
```

関連コマンド

config boot

show band-select

帯域幅選択情報を表示するには、**show band-select** コマンドを使用します。

show band-select

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show band-select** コマンドの出力例を示します。

```
(Cisco Controller) > show band-select
Band Select Probe Response..................... per WLAN enabling
   Cycle Count................................. 3 cycles
   Cycle Threshold............................. 200 milliseconds
   Age Out Suppression......................... 20 seconds
   Age Out Dual Band........................... 60 seconds
   Client RSSI................................. -80 dBm
```

関連コマンド

config band-select

config wlan band-select

show buffers

コントローラのバッファ情報を表示するには、**show buffers** コマンドを使用します。

show buffers

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show buffers** コマンドの出力例を示します。

```
(Cisco Controller) > show buffers
Pool[00]: 16 byte chunks
    chunks in pool:    50000
    chunks in use:     9196
    bytes in use:      147136
    bytes requested:   73218 (73918 overhead bytes)
Pool[01]: 64 byte chunks
    chunks in pool:    50100
    chunks in use:     19222
    bytes in use:      1230208
    bytes requested:   729199 (501009 overhead bytes)
Pool[02]: 128 byte chunks
    chunks in pool:    26200
    chunks in use:     9861
    bytes in use:      1262208
    bytes requested:   848732 (413476 overhead bytes)
Pool[03]: 256 byte chunks
    chunks in pool:    3000
    chunks in use:     596
    bytes in use:      152576
    bytes requested:   93145 (59431 overhead bytes)
Pool[04]: 384 byte chunks
    chunks in pool:    6000
    chunks in use:     258
    bytes in use:      99072
    bytes requested:   68235 (30837 overhead bytes)
Pool[05]: 512 byte chunks
    chunks in pool:    18700
    chunks in use:     18667
    bytes in use:      9557504
    bytes requested:   7933814 (1623690 overhead bytes)
Pool[06]: 1024 byte chunks
    chunks in pool:    3500
    chunks in use:     94
    bytes in use:      96256
    bytes requested:   75598 (20658 overhead bytes)
Pool[07]: 2048 byte chunks
    chunks in pool:    1000
    chunks in use:     54
    bytes in use:      110592
```

```
    bytes requested:   76153 (34439 overhead bytes)
Pool[08]: 4096 byte chunks
    chunks in pool:    1000
    chunks in use:     47
    bytes in use:      192512
    bytes requested:   128258 (64254 overhead bytes)
Raw Pool:
    chunks in use:     256
    bytes requested:   289575125
```

show cac voice stats

802.11a または 802.11b 無線の詳細な音声 CAC 統計情報を表示するには、**show cac voice stats** コマンドを使用します。

show cac voice stats {**802.11a** | **802.11b**}

構文の説明

802.11a	802.11a の詳細な音声 CAC 統計情報を表示します。
802.11b	802.11b/g の詳細な音声 CAC 統計情報を表示します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show cac voice stats 802.11b** コマンドの出力例を示します。

```
(Cisco Controller) > show cac voice stats 802.11b

WLC Voice Call Statistics for 802.11b Radio

WMM TSPEC CAC Call Stats
  Total num of Calls in progress.................. 0
  Num of Roam Calls in progress.................. 0
  Total Num of Calls Admitted.................... 0
  Total Num of Roam Calls Admitted............... 0
  Total Num of exp bw requests received.......... 0
  Total Num of exp bw requests Admitted.......... 0
  Total Num of Calls Rejected.................... 0
  Total Num of Roam Calls Rejected............... 0
  Num of Calls Rejected due to insufficent bw.... 0
  Num of Calls Rejected due to invalid params.... 0
  Num of Calls Rejected due to PHY rate.......... 0
  Num of Calls Rejected due to QoS policy........ 0
SIP CAC Call Stats
  Total Num of Calls in progress.................. 0
  Num of Roam Calls in progress.................. 0
  Total Num of Calls Admitted.................... 0
  Total Num of Roam Calls Admitted............... 0
  Total Num of Preferred Calls Received.......... 0
  Total Num of Preferred Calls Admitted.......... 0
  Total Num of Ongoing Preferred Calls........... 0
  Total Num of Calls Rejected(Insuff BW)......... 0
  Total Num of Roam Calls Rejected(Insuff BW).... 0
KTS based CAC Call Stats
  Total Num of Calls in progress.................. 0
  Num of Roam Calls in progress.................. 0
  Total Num of Calls Admitted.................... 0
  Total Num of Roam Calls Admitted............... 0
  Total Num of Calls Rejected(Insuff BW)......... 0
  Total Num of Roam Calls Rejected(Insuff BW).... 0
```

show cac voice summary

短い音声統計を含むすべての AP のリストを表示するには（使用帯域幅、使用可能な最大帯域幅、およびコール数など）、**show cac voice summary** コマンドを使用します。

show cac voice summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show cac voice summary** コマンドの出力例を示します。

```
(Cisco Controller) > show cac voice summary
    AP Name         Slot#   Radio  BW Used/Max  Calls
-----------------  -------  -----  -----------  -----
APc47d.4f3a.3547     0      11b/g     0/23437    0
      1      11a    1072/23437    1
```

show cac video stats

802.11a または 802.11b 無線の詳細な音声 CAC 統計情報を表示するには、**show cac video stats** コマンドを使用します。

show cac video stats {**802.11a** | **802.11b**}

構文の説明

802.11a	802.11a の詳細なビデオ CAC 統計情報を表示します。
802.11b	802.11b/g. の詳細なビデオCAC統計情報を表示します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show cac video stats 802.11b** コマンドの出力例を示します。

```
(Cisco Controller) > show cac video stats 802.11b

WLC Video Call Statistics for 802.11b Radio

WMM TSPEC CAC Call Stats
  Total num of Calls in progress.................. 0
  Num of Roam Calls in progress.................. 0
  Total Num of Calls Admitted.................... 0
  Total Num of Roam Calls Admitted............... 0
  Total Num of Calls Rejected.................... 0
  Total Num of Roam Calls Rejected............... 0
  Num of Calls Rejected due to insufficent bw.... 0
  Num of Calls Rejected due to invalid params.... 0
  Num of Calls Rejected due to PHY rate.......... 0
  Num of Calls Rejected due to QoS policy........ 0
SIP CAC Call Stats
  Total Num of Calls in progress.................. 0
  Num of Roam Calls in progress.................. 0
  Total Num of Calls Admitted.................... 0
  Total Num of Roam Calls Admitted............... 0
  Total Num of Calls Rejected(Insuff BW)......... 0
  Total Num of Roam Calls Rejected(Insuff BW).... 0
```

関連コマンド

config 802.11 cac voice

config 802.11 cac defaults

config 802.11 cac video

config 802.11 cac multimedia

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video load-based

config 802.11 cac video cac-method

config 802.11 cac video sip

show cac video summary

短いビデオ統計情報を含むすべてのアクセスポイントのリストを表示するには（使用帯域幅、使用可能な最大帯域幅、およびコール数など）、**show cac video summary** コマンドを使用します。

show cac video summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、**show cac video summary** コマンドの出力例を示します。

```
(Cisco Controller) > show cac video summary

    AP Name          Slot#   Radio  BW Used/Max  Calls
-----------------  -------  -----  -----------  -----
AP001b.d571.88e0     0      11b/g     0/10937    0
                     1      11a       0/18750    0
AP5_1250             0      11b/g     0/10937    0
                     1      11a       0/18750    0
```

関連コマンド

config 802.11 cac voice

config 802.11 cac defaults

config 802.11 cac video

config 802.11 cac multimedia

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video load-based

config 802.11 cac video cac-method

config 802.11 cac video sip

show call-control ap

（注） **show call-control ap** コマンドは SIP ベースのコールにのみ適用されます。

成功したコールのメトリックまたは失敗したコールについて生成されたトラップを確認するには、**show call-control ap** コマンドを使用します。

show call-control ap {**802.11a** | **802.11b**} *cisco_ap* {**metrics** | **traps**}

構文の説明

802.11a	802.11a ネットワークを指定します
802.11b	802.11b/g ネットワークを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
metrics	コール メトリックの情報を指定します。
traps	コール制御にトラップ情報を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

トラブルシューティングに役立つように、このコマンドの出力には失敗したコールすべてのエラー コードが示されます。次の表では、失敗したコールの考えられるエラー コードについて説明します。

表 *11* : 失敗した *Voice over IP*（*VoIP*）コールのエラー コード

エラー コード	整数	説明
1	unknown	不明なエラー。
400	badRequest	構文が不正であるため要求を認識できませんでした。
401	unauthorized	要求にはユーザ認証が必要です。
402	paymentRequired	将来的な使用のために予約されています。

エラー コード	整数	説明
403	forbidden	サーバは要求を認識しましたが、実行を拒否しています。
404	notFound	サーバは、このユーザが Request-URI に指定されたドメインに存在しないという情報を持っています。
405	methodNotallowed	Request-Line で指定されたメソッドが認識されているものの、Request-URI で指定されたアドレスでは許可されていません。
406	notAcceptable	要求によって指定されたリソースは、送信された要求内の [Accept] ヘッダー フィールドによって許容されないコンテンツ特性を持つ応答エンティティしか生成できません。
407	proxyAuthenticationRequired	クライアントは、最初にプロキシで認証される必要があります。
408	requestTimeout	サーバは、適切な時間内に応答を生成できませんでした。
409	conflict	リソースの現在の状態と競合したために、要求を完了できませんでした。
410	gone	要求されたリソースがサーバで使用できず、転送アドレスが不明です。
411	lengthRequired	要求のエンティティ自体が、サーバが処理を想定しているサイズ、または処理できるサイズより大きいため、サーバが要求の処理を拒否しています。

エラー コード	整数	説明
413	requestEntityTooLarge	要求のエンティティ自体が、サーバが処理を想定しているサイズ、または処理できるサイズより大きいため、サーバが要求の処理を拒否しています。
414	requestURITooLarge	Request-URI がサーバが解釈を想定している長さよりも長いために、サーバが要求の処理を拒否しています。
415	unsupportedMediaType	要求されたメソッドについて、要求のメッセージ本文の形式がサーバでサポートされていないために、サーバが要求の処理を拒否しています。
420	badExtension	Proxy-Require または Require ヘッダー フィールドで指定されたプロトコル拡張が、サーバで認識されませんでした。
480	temporarilyNotAvailable	着信側のエンド システムが正常に通信できるものの、着信側が現在、利用不能です。
481	callLegDoesNotExist	User-Agent Server（UAS; ユーザ エージェント サーバ）が既存のダイアログまたはトランザクションと一致していない要求を受け取りました。
482	loopDetected	サーバはループを検出しました。
483	tooManyHops	サーバは Max-Forwards ヘッダー フィールドの値が 0 である要求を受信しました。
484	addressIncomplete	サーバは Request-URI が不完全である要求を受信しました。
485	ambiguous	Request-URI があいまいです。

エラー コード	整数	説明
486	busy	着信側のエンド システムは正常に接続されましたが、着信側は現在、このエンド システムで追加のコールを受け入れようとしないか、受け入れることができません。
500	internalServerError	サーバで、要求の処理を妨げる予期しない状態が発生しました。
501	notImplemented	サーバは要求を処理するために必要な機能をサポートしていません。
502	badGateway	ゲートウェイまたはプロキシとして機能しているサーバが、要求を処理するためにアクセスしたダウンストリーム サーバから無効な応答を受信しました。
503	serviceUnavailable	一時的な過負荷またはメンテナンスのために、サーバが一時的に要求を処理できなくなっています。
504	serverTimeout	サーバは、要求を処理するためにアクセスした外部サーバから時間内に応答を受信しませんでした。
505	versionNotSupported	サーバは、要求で使用された SIP プロトコルのバージョンをサポートしていないか、サポートを拒否しています。
600	busyEverywhere	着信側のエンド システムは正常に接続されましたが、着信側はこの時点でビジーであるか、コールに応答しようとしていません。

エラー コード	整数	説明
603	decline	着信側のマシンは正常に接続されましたが、ユーザが参加しようとしていないか、参加できません。
604	doesNotExistAnywhere	サーバには、Request-URI で示されたユーザが存在しないという情報があります。
606	notAcceptable	ユーザのエージェントは正常に接続されましたが、セッションの説明の一部（要求されるメディア、帯域幅、アドレス指定形式など）が受け入れられませんでした。

次に、アクセス ポイントに対して生成された、成功したコールを表示する **show call-controller ap** コマンドの出力例を示します。

```
(Cisco Controller) >show call-control ap 802.11a Cisco_AP metrics
Total Call Duration in Seconds..................... 120
Number of Calls.................................... 10
Number of calls for given client is................ 1
```

次に、AP に対して生成された、トラップのメトリックを表示する **show call-control ap** コマンドの出力例を示します。

```
(Cisco Controller) >show call-control ap 802.11a Cisco_AP traps
Number of traps sent in one min.................... 2
Last SIP error code................................ 404
Last sent trap timestamp...................... Jun 20 10:05:06
```

show call-control client

Voice-over-IP（VoIP）スヌーピングがイネーブルになっており、コールがアクティブである場合に、コールを認識するクライアントのコール情報を確認するには、**show call-control client** コマンドを使用します。

show call-control client callInfo *client_MAC_address*

構文の説明

callInfo	コール制御情報を指定します。
client_MAC_address	クライアント MAC アドレス

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show call-controller client** コマンドの出力例を示します。

```
(Cisco Controller) > show call-control client callInfo 10.10.10.10.10.10
Uplink IP/port................................. 0.0.0.0 /   0
Downlink  IP/port.............................. 9.47.96.107 / 5006
UP.............................................   6
Calling Party.................................. sip:1021
Called Party................................... sip:1000
Call ID........................................ 38423970c3fca477
Call on hold: ................................. FALSE
Number of calls for given client is.............. 1
```

show call-home summary

Call Home の詳細を表示するには、**show call-home summary** コマンドを使用します。

show call-home summary

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home サマリーの例を示します。

```
(Cisco Controller) > show call-home summaryCurrent call home settings:
    call home feature : enabled
    contact person's email address: sch-smart-licensing@cisco.com

    Mail-server: Not yet set up
    http proxy: Not yet set up


    Smart licensing messages: disabled

    data-privacy: normal
    Event throttling: Off

    Rate-limit: 20 message(s) per minute
Profile name:  CiscoTAC-1
   Status: Inactive
   TAC profile: Yes
   Mode: Full reporting
   Report data: SCH SL
   Msg Format: XML
   Msg size limit: 3145728
   Transport method: HTTP

--More-- or (q)uit In slWlcProcessSLStatsClearMsg
      https://tools.cisco.com/its/service/oddce/services/DDCEService
```

show capwap reap association

アクセス ポイントにアソシエートされているクライアントとそのサービス セット ID（SSID）のリストを表示するには、**show capwap reap association** コマンドを使用します。

show capwap reap association

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントにアソシエートされているクライアントとその SSID を表示する例を示します。

```
(Cisco Controller) >show capwap reap association
```

show capwap reap status

FlexConnect アクセス ポイントのステータス（connected または standalone）を表示するには、**show capwap reap status** コマンドを使用します。

show capwap reap status

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

AP 固有として設定されている場合、コマンドは VLAN のみを表示します。

次に、FlexConnect アクセス ポイントのステータスを表示する例を示します。

```
(Cisco Controller) >show capwap reap status
```

show cdp

Cisco Discovery Protocol（CDP）のステータスと詳細を表示するには、**show cdp** コマンドを使用します。

show cdp {**neighbors**［**detail**］ | **entry all** | **traffic**}

構文の説明

neighbors	すべてのインターフェイスのすべての CDP ネイバーのリストを表示します。
detail	（任意）コントローラの CDP ネイバーに関する詳細情報を表示します。このコマンドは、コントローラの CDP ネイバーのみを表示します。コントローラに関連付けられたアクセス ポイントの CDP ネイバーは表示しません。
entry all	データベース内のすべての CDP エントリを表示します。
traffic	CDP トラフィック情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show cdp** コマンドの出力例を示します。

```
(Cisco Controller) > show cdp
CDP counters :
Total packets output: 0, Input: 0
Chksum error: 0
No memory: 0, Invalid packet: 0,
```

関連コマンド

config cdp

config ap cdp

show ap cdp

show certificate compatibility

Cisco Wireless LAN Controller で証明書の適合性が確認されているかどうかを表示するには、**show certificate compatibility** コマンドを使用します。

show certificate compatibility

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show certificate compatibility** コマンドの出力例を示します。

```
(Cisco Controller) > show certificate compatibility
Certificate compatibility mode:.............. off
```

show certificate lsc

コントローラによってローカルで有効な証明書（LSC）が生成されたことを確認するには、**show certificate lsc summary** コマンドを使用します。

show certificate lsc {**summary** | **ap-provision**}

構文の説明

summary	LSC 証明書設定および証明書の要約を表示します。
ap-provision	LSC を使用してプロビジョニングされるアクセス ポイントに関する詳細を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show certificate lsc summary** コマンドの出力例を示します。

```
(Cisco Controller) > show certificate lsc summary
LSC Enabled..................................... Yes
LSC CA-Server................................... http://10.0.0.1:8080/caserver
LSC AP-Provisioning............................. Yes
Provision-List.............................. Not Configured
LSC Revert Count in AP reboots.............. 3
LSC Params:
Country..................................... 4
State....................................... ca
City........................................ ss
Orgn........................................ org
Dept........................................ dep
Email....................................... dep@co.com
KeySize..................................... 390
LSC Certs:
CA Cert..................................... Not Configured
RA Cert..................................... Not Configured
```

次に、LSC を使用してプロビジョニングされるアクセス ポイントに関する詳細を表示する例を示します。

```
(Cisco Controller) > show certificate lsc ap-provision
LSC AP-Provisioning............................. Yes
Provision-List.................................. Present
Idx Mac Address
--- -------------
1 00:18:74:c7:c0:90
```

show certificate ssc

Self Signed Device Certificate（SSC）と仮想コントローラのハッシュ キーを表示するには、**show certificate ssc** コマンドを使用します。

show certificate ssc

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show certificate ssc** コマンドの出力例を示します。

```
(Cisco Controller) > show certificate ssc
 SSC Hash validation..............................Enabled.

 SSC Device Certificate details:

         Subject Name :
               C=US, ST=California, L=San Jose, O=Cisco Virtual Wireless LAN Controller,

                 CN=DEVICE-vWLC-AIR-CTVM-K9-000C297F2CF7, MAILTO=support@vwlc.com

         Validity :
                 Start : 2012 Jul 23rd, 15:47:53 GMT
                 End   : 2022 Jun  1st, 15:47:53 GMT

         Hash key : 5870ffabb15de2a617132bafcd73
```

show certificate summary

コントローラにより証明書が生成されたことを確認するには、**show certificate summary** コマンドを使用します。

show certificate summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show certificate summary** コマンドの出力例を示します。

```
(Cisco Controller) > show certificate summary
Web Administration Certificate..... Locally Generated
Web Authentication Certificate..... Locally Generated
Certificate compatibility mode:..... off
```

show client ap

Cisco Lightweight アクセス ポイント上のクライアントを表示するには、**show client ap** コマンドを使用します。

show client ap 802.11{**a** | **b**} *cisco_ap*

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b/g ネットワークを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

なし

使用上のガイドライン

show client ap コマンドは自動的に無効にされたクライアントのステータスを表示できます。**show exclusionlist** コマンドを使用して、除外リスト（ブラックリスト）上のクライアントを表示します。

次に、アクセス ポイント上のクライアント情報を表示する例を示します。

```
(Cisco Controller) >show client ap 802.11b AP1
MAC Address        AP Id   Status         WLAN Id    Authenticated
-----------------  ------  -------------  ---------  -------------
xx:xx:xx:xx:xx:xx      1   Associated     1          No
```

show client calls

コントローラ上のアクティブなコールまたは拒否されたコールの合計数を表示するには、**show client calls** コマンドを使用します。

show client calls {**active** | **rejected**} {**802.11a** | **802.11bg** | **all**}

構文の説明

active	アクティブなコールを指定します。
rejected	拒否されたコールを指定します。
802.11a	802.11a ネットワークを指定します。
802.11bg	802.11b/g ネットワークを指定します。
all	802.11a および 802.11b/g ネットワークの両方を指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client calls active 802.11a** コマンドの出力例を示します。

```
(Cisco Controller) > show client calls active 802.11a
Client MAC              Username         Total Call            AP Name         Radio
Type
                                        Duration (sec)
--------------------    ---------       ----------      ---------------     ----------
00:09: ef: 02:65:70       abc              45           VJ-1240C-ed45cc       802.11a
00:13: ce: cc: 51:39      xyz              45               AP1130-a416       802.11a
00:40:96: af: 15:15       def              45               AP1130-a416       802.11a
00:40:96:b2:69: df        def              45               AP1130-a416       802.11a
Number of Active Calls ------------------------------------ 4
```

show client ccx client-capability

クライアントの機能情報を表示するには、**show client ccx client-capability** コマンドを使用します。

show client ccx client-capability *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドはクライアントで使用可能な機能を表示します。機能の現在の設定ではありません。

次に、**show client ccx client-capability** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx client-capability 00:40:96:a8:f7:98
Service Capability..................................... Voice, Streaming(uni-directional)
Video, Interactive(bi-directional) Video
Radio Type............................................. DSSS OFDM(802.11a) HRDSSS(802.11b)
 ERP(802.11g)
Radio Type............................................. DSSS
 Radio Channels..................................... 1 2 3 4 5 6 7 8 9 10 11
 Tx Power Mode...................................... Automatic
 Rate List(MB)...................................... 1.0 2.0
Radio Type............................................. HRDSSS(802.11b)
 Radio Channels..................................... 1 2 3 4 5 6 7 8 9 10 11
 Tx Power Mode...................................... Automatic
 Rate List(MB)...................................... 5.5 11.0
Radio Type............................................. ERP(802.11g)
 Radio Channels..................................... 1 2 3 4 5 6 7 8 9 10 11
 Tx Power Mode...................................... Automatic
 Rate List(MB)...................................... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Are you sure you want to start? (y/N)y Are you sure you want to start? (y/N)
```

show client ccx frame-data

最後のテストについて、クライアントから送信されたデータ フレームを表示するには、**show client ccx frame-data** コマンドを使用します。

show client ccx frame-data *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx frame-data** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx frame-data
 xx:xx:xx:xx:xx:xx
```

show client ccx last-response-status

最後のテスト応答のステータスを表示するには、**show client ccx last-response-status** コマンドを使用します。

show client ccx last-response-status *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx last-response-status** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx last-response-status
Test Status ....................... Success
Response Dialog Token.............. 87
Response Status.................... Successful
Response Test Type................. 802.1x Authentication Test
Response Time...................... 3476 seconds since system boot
```

show client ccx last-test-status

最後のテストのステータスを表示するには、**show client ccx last-test-status** コマンドを使用します。

show client ccx last-test-status *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx last-test-status** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx last-test-status

Test Type ....................... Gateway Ping Test
Test Status ..................... Pending/Success/Timeout
Dialog Token .................... 15
Timeout ......................... 15000 ms
Request Time .................... 1329 seconds since system boot
```

show client ccx log-response

ログ応答を表示するには、**show client ccx log-response** コマンドを使用します。

show client ccx log-response {**roam** | **rsna** | **syslog**} *client_mac_address*

構文の説明

roam	（任意）CCXクライアントのローミング ログ応答を表示します。
rsna	（任意）CCX クライアントの RSNA ログ応答を表示します。
syslog	（任意）CCXクライアントのシステム ログ応答を表示します。
client_mac_address	指定したアクセス ポイントのインベントリ。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx log-response syslog** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx log-response syslog 00:40:96:a8:f7:98
Tue Jun 26 18:07:48 2007       Syslog Response LogID=131: Status=Successful
        Event Timestamp=0d 00h 19m 42s 278987us
       Client SysLog = '<11> Jun 19 11:49:47 unraval13777 Mandatory elements missing in
 the OID response'
       Event Timestamp=0d 00h 19m 42s 278990us
       Client SysLog = '<11> Jun 19 11:49:47 unraval13777 Mandatory elements missing in
 the OID response'
Tue Jun 26 18:07:48 2007       Syslog Response LogID=131: Status=Successful
        Event Timestamp=0d 00h 19m 42s 278987us
       Client SysLog = '<11> Jun 19 11:49:47 unraval13777 Mandatory elements missing in
 the OID response'
       Event Timestamp=0d 00h 19m 42s 278990us
       Client SysLog = '<11> Jun 19 11:49:47 unraval13777 Mandatory elements missing in
 the OID response'
```

次に、クライアントのローミング ログ応答を表示する例を示します。

```
(Cisco Controller) >show client ccx log-response roam 00:40:96:a8:f7:98
Thu Jun 22 11:55:14 2007    Roaming Response LogID=20: Status=Successful
Event Timestamp=0d 00h 00m 13s 322396us      Source BSSID=00:40:96:a8:f7:98
Target BSSID=00:0b:85:23:26:70,      Transition Time=100(ms)
Transition Reason: Normal roam, poor link      Transition Result: Success
Thu Jun 22 11:55:14 2007    Roaming Response LogID=133: Status=Successful
Event Timestamp=0d 00h 00m 16s 599006us      Source BSSID=00:0b:85:81:06:c2
Target BSSID=00:0b:85:81:06:c2,      Transition Time=3235(ms)
Transition Reason: Normal roam, poor link      Transition Result: Success
Thu Jun 22 18:28:48 2007    Roaming Response LogID=133: Status=Successful
```

```
Event Timestamp=0d 00h 00m 08s 815477us      Source BSSID=00:0b:85:81:06:c2
Target BSSID=00:0b:85:81:06:d2,      Transition Time=3281(ms)
Transition Reason: First association to WLAN      Transition Result: Success
```

show client ccx manufacturer-info

クライアントの製造情報を表示するには、**show client ccx manufacturer-info** コマンドを使用します。

show client ccx manufacturer-info *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx manufacturer-info** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx manufacturer-info 00:40:96:a8:f7:98
Manufacturer OUI ............................. 00:40:96
Manufacturer ID .............................. Cisco
Manufacturer Model ........................... Cisco Aironet 802.11a/b/g Wireless Adapter
Manufacturer Serial .......................... FOC1046N3SX
Mac Address .................................. 00:40:96:b2:8d:5e
Radio Type ................................... DSSS OFDM(802.11a) HRDSSS(802.11b)
  ERP(802.11g)
Antenna Type ................................. Omni-directional diversity
Antenna Gain ................................. 2 dBi
Rx Sensitivity:
Radio Type ................................... DSSS
Rx Sensitivity ................................ Rate:1.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ................................ Rate:2.0 Mbps, MinRssi:-95, MaxRss1:-30
Radio Type ................................... HRDSSS(802.11b)
Rx Sensitivity ................................ Rate:5.5 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ................................ Rate:11.0 Mbps, MinRssi:-95, MaxRss1:-30
Radio Type ................................... ERP(802.11g)
Rx Sensitivity ................................ Rate:6.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ................................ Rate:9.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ................................ Rate:12.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ................................ Rate:18.0 Mbps, MinRss1:-95, MaxRss1:-30
```

show client ccx operating-parameters

クライアントの動作パラメータを表示するには、**show client ccx operating-parameters** コマンドを使用します。

show client ccx operating-parameters *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx operating-parameters** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx operating-parameters 00:40:96:b2:8d:5e
Client Mac ..................................... 00:40:96:b2:8d:5e
Radio Type ..................................... OFDM(802.11a)
Radio Type ..................................... OFDM(802.11a)
 Radio Channels ................................ 36 40 44 48 52 56 60 64 100 104 108
112 116 120 124 128 132 136 140 149 153 157 161 165
 Tx Power Mode ................................ Automatic
 Rate List(MB)................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Power Save Mode ................................ Normal Power Save
SSID ........................................... wifi
Security Parameters[EAP Method, Credential]..... None
Auth Method .................................... None
Key Management.................................. None
Encryption ..................................... None
Device Name .................................... Wireless Network Connection 15
Device Type .................................... 0
OS Id .......................................... Windows XP
OS Version ..................................... 5.1.6.2600 Service Pack 2
IP Type ........................................ DHCP address
IPv4 Address ................................... Available
IP Address ..................................... 70.0.4.66
Subnet Mask .................................... 255.0.0.0
Default Gateway ................................ 70.1.0.1
IPv6 Address ................................... Not Available
IPv6 Address ................................... 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
IPv6 Subnet Mask ............................... 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
DNS Servers .................................... 103.0.48.0
WINS Servers ...................................
System Name .................................... URAVAL3777
Firmware Version ............................... 4.0.0.187
Driver Version ................................. 4.0.0.187
```

show client ccx profiles

クライアント プロファイルを表示するには、**show client ccx profiles** コマンドを使用します。

show client ccx profiles *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx profiles** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx profiles 00:40:96:15:21:ac
Number of Profiles ................................ 1
Current Profile ................................... 1
Profile ID ........................................ 1
Profile Name ...................................... wifiEAP
SSID .............................................. wifiEAP
Security Parameters [EAP Method, Credential]..... EAP-TLS, Host OS Login Credentials
Auth Method ....................................... EAP
Key Management .................................... WPA2+CCKM
Encryption ........................................ AES-CCMP
Power Save Mode ................................... Constantly Awake
Radio Configuration:
Radio Type..................................... DSSS
 Preamble Type................................. Long preamble
 CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
 Data Retries.................................. 6
 Fragment Threshold............................ 2342
 Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
 Tx Power Mode................................. Automatic
 Rate List (MB)................................ 1.0 2.0
Radio Type..................................... HRDSSS(802.11b)
 Preamble Type................................. Long preamble
 CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
 Data Retries.................................. 6
 Fragment Threshold............................ 2342
 Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
 Tx Power Mode................................. Automatic
 Rate List(MB)................................. 5.5 11.0
Radio Type..................................... ERP(802.11g)
 Preamble Type................................. Long preamble
 CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
 Data Retries.................................. 6
 Fragment Threshold............................ 2342
 Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
 Tx Power Mode................................. Automatic
 Rate List (MB)................................ 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Radio Type..................................... OFDM(802.11a)
 Preamble Type................................. Long preamble
```

```
 CCA Method..................................... Energy Detect + Carrier
Detect/Correlation
 Data Retries................................... 6
 Fragment Threshold............................. 2342
 Radio Channels................................. 36 40 44 48 52 56 60 64 149 153 157
161 165
 Tx Power Mode.................................. Automatic
 Rate List (MB)................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
```

show client ccx results

最後に正常終了した診断テストの結果を表示するには、**show client ccx results** コマンドを使用します。

show client ccx results *client_mac_address*

構文の説明

client_mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx results** コマンドの出力例を示します。

```
(Cisco Controller) >show client ccx results xx.xx.xx.xx
dot1x Complete..................................... Success
EAP Method......................................... *1,Host OS Login Credentials
dot1x Status....................................... 255
```

show client ccx rm

Cisco Client eXtension（CCX）クライアントの無線管理レポート情報を表示するには、**show client ccx rm** コマンドを使用します。

show client ccx rm *client_MAC* {**status** | {**report** {**chan-load** | **noise-hist** | **frame** | **beacon** | **pathloss**}}}

構文の説明

client_MAC	クライアント MAC アドレス
status	クライアントのCCX無線管理ステータス情報を表示します。
report	クライアントのCCX無線管理レポートを表示します。
chan-load	無線管理チャネル ロード レポートを表示します。
noise-hist	無線管理ノイズ ヒストグラム レポートを表示します。
beacon	無線管理ビーコン ロード レポートを表示します。
frame	無線管理フレーム レポートを表示します。
pathloss	無線管理パス損失レポートを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアント無線管理ステータス情報を表示する例を示します。

```
(Cisco Controller) >show client ccx rm 00:40:96:15:21:ac status

Client Mac Address.............................. 00:40:96:15:21:ac
Channel Load Request............................ Enabled
Noise Histogram Request......................... Enabled
Beacon Request.................................. Enabled
Frame Request................................... Enabled
Interval........................................ 30
Iteration....................................... 10
```

次に、クライアント無線管理ロード レポートを表示する例を示します。

```
(Cisco Controller) >show client ccx rm 00:40:96:15:21:ac report chan-load

Channel Load Report
Client Mac Address.............................. 00:40:96:ae:53:bc
Timestamp....................................... 788751121
Incapable Flag.................................. On
Refused Flag.................................... On
Chan CCA Busy Fraction
-----------------------
1  194
2  86
3  103
4  0
5  178
6  82
7  103
8  95
9  13
10 222
11 75
```

次に、クライアント無線管理ノイズヒストグラム レポートを表示する例を示します。

```
(Cisco Controller) >show client ccx rm 00:40:96:15:21:ac report noise-hist

Noise Histogram Report
Client Mac Address.............................. 00:40:96:15:21:ac
Timestamp....................................... 4294967295
Incapable Flag.................................. Off
Refused Flag.................................... Off
Chan RPI0 RPI1 RPI2 RPI3 RPI4 RPI5 RPI6 RPI7
```

show client ccx stats-report

指定されたクライアントデバイスからのCisco Client eXtensions（CCX）統計情報レポートを表示するには、**show client ccx stats-report** コマンドを使用します。

show client ccx stats-report *client_mac_address*

構文の説明

client_mac_address	クライアント MAC アドレス

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client ccx stats-report** コマンドの出力例を示します。

```
(Cisco Controller) > show client ccx stats-report 00:0c:41:07:33:a6
Measurement duration = 1
dot11TransmittedFragmentCount       = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount                    = 3
dot11RetryCount                     = 4
dot11MultipleRetryCount             = 5
dot11FrameDuplicateCount            = 6
dot11RTSSuccessCount                = 7
dot11RTSFailureCount                = 8
dot11ACKFailureCount                = 9
dot11ReceivedFragmentCount          = 10
dot11MulticastReceivedFrameCount    = 11
dot11FCSErrorCount                  = 12
dot11TransmittedFrameCount          = 13
```

show client detail

DNS スヌーピング（DNS ベースの ACL）によって学習されたクライアントごとの IP アドレスを表示するには、**show client detail** *mac_address* コマンドを使用します。

show client detail *mac_address*

構文の説明

mac_address	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。

次に、**show client detail** *mac_address* コマンドの出力例を示します。

```
(Cisco Controller) > show client detail 01:35:6x:yy:21:00
 Client MAC Address.............................. 01:35:6x:yy:21:00
Client Username ................................ test
AP MAC Address.................................. 00:11:22:33:44:x0
AP Name......................................... AP0011.2020.x111
AP radio slot Id................................ 1
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 7
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:11:22:33:44:xx
Connected For .................................. 28 secs
Channel......................................... 56
IP Address...................................... 10.0.0.1
Gateway Address................................. Unknown
Netmask......................................... Unknown
IPv6 Address.....................................
xx20::222:6xyy:zeeb:2233
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0
Client CCX version.............................. No CCX support
Re-Authentication Timeout....................... 1756
QoS Level....................................... Silver
Avg data Rate................................... 0
Burst data Rate................................. 0
Avg Real time data Rate......................... 0
Burst Real Time data Rate....................... 0
802.1P Priority Tag............................. disabled
```

```
CTS Security Group Tag.......................... Not Applicable
KTS CAC Capability.............................. No
WMM Support..................................... Enabled
  APSD ACs.....................................  BK  BE  VI  VO
Power Save...................................... ON
Current Rate.................................... m7
Supported Rates.................................
6.0,9.0,12.0,18.0,24.0,36.0,
    ........................................... 48.0,54.0
Mobility State.................................. Local
Mobility Move Count............................. 0
Security Policy Completed....................... No
Policy Manager State........................... SUPPLICANT_PROVISIONING
Policy Manager Rule Created..................... Yes
AAA Override ACL Name........................... android
AAA Override ACL Applied Status................. Yes
AAA Override Flex ACL Name...................... none
AAA Override Flex ACL Applied Status............ Unavailable
AAA URL redirect................................
https://10.0.0.3:8443/guestportal/gateway?sessionId=0a68aa72000000015272404e&action=nsp
Audit Session ID................................
0a68aa72000000015272404e
AAA Role Type................................... none
Local Policy Applied............................ p1
IPv4 ACL Name................................... none
FlexConnect ACL Applied Status.................. Unavailable
IPv4 ACL Applied Status......................... Unavailable
IPv6 ACL Name................................... none
IPv6 ACL Applied Status......................... Unavailable
Layer2 ACL Name................................. none
Layer2 ACL Applied Status....................... Unavailable
Client Type..................................... SimpleIP
mDNS Status..................................... Enabled
mDNS Profile Name.............................. default-mdns-profile
No. of mDNS Services Advertised................. 0
Policy Type..................................... WPA2
Authentication Key Management................... 802.1x
Encryption Cipher............................... CCMP (AES)
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type........................................ PEAP
Interface.......................................
.. management
VLAN............................................ 0
Quarantine VLAN................................. 0
Access VLAN..................................... 0
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Not implemented
      PBCC...................................... Not implemented
```

```
      Channel Agility.......................... Not implemented
      Listen Interval.......................... 10
      Fast BSS Transition...................... Not implemented
Client Wifi Direct Capabilities:
      WFD capable.............................. No
      Manged WFD capable....................... No
      Cross Connection Capable................. No
      Support Concurrent Operation............. No
Fast BSS Transition Details:
Client Statistics:
      Number of Bytes Received................. 123659
      Number of Bytes Sent..................... 120564
      Number of Packets Received............... 1375
      Number of Packets Sent................... 276
      Number of Interim-Update Sent............ 0
      Number of EAP Id Request Msg Timeouts..... 0
      Number of EAP Id Request Msg Failures..... 0
      Number of EAP Request Msg Timeouts........ 2
      Number of EAP Request Msg Failures........ 0
      Number of EAP Key Msg Timeouts............ 0
      Number of EAP Key Msg Failures............ 0
      Number of Data Retries................... 82
      Number of RTS Retries.................... 0
      Number of Duplicate Received Packets..... 0
      Number of Decrypt Failed Packets......... 0
      Number of Mic Failured Packets........... 0
      Number of Mic Missing Packets............ 0
      Number of RA Packets Dropped............. 0
      Number of Policy Errors.................. 0
      Radio Signal Strength Indicator.......... -51 dBm
      Signal to Noise Ratio.................... 46 dB
Client Rate Limiting Statistics:
      Number of Data Packets Recieved.......... 0
      Number of Data Rx Packets Dropped........ 0
      Number of Data Bytes Recieved............ 0
      Number of Data Rx Bytes Dropped.......... 0
      Number of Realtime Packets Recieved...... 0
      Number of Realtime Rx Packets Dropped.... 0
      Number of Realtime Bytes Recieved........ 0
      Number of Realtime Rx Bytes Dropped...... 0
      Number of Data Packets Sent.............. 0
      Number of Data Tx Packets Dropped........ 0
      Number of Data Bytes Sent................ 0
      Number of Data Tx Bytes Dropped.......... 0
      Number of Realtime Packets Sent.......... 0
      Number of Realtime Tx Packets Dropped.... 0
      Number of Realtime Bytes Sent............ 0
      Number of Realtime Tx Bytes Dropped...... 0
Nearby AP Statistics:
      AP0022.9090.c545(slot 0)
        antenna0: 26 secs ago.................. -33 dBm
```

```
        antenna1: 26 secs ago..................... -35 dBm
      AP0022.9090.c545(slot 1)
        antenna0: 25 secs ago..................... -41 dBm
        antenna1: 25 secs ago..................... -44 dBm
      APc47d.4f3a.35c2(slot 0)
        antenna0: 26 secs ago..................... -30 dBm
        antenna1: 26 secs ago..................... -36 dBm
      APc47d.4f3a.35c2(slot 1)
        antenna0: 24 secs ago..................... -43 dBm
        antenna1: 24 secs ago..................... -45 dBm
DNS Server details:
      DNS server IP ............................. 0.0.0.0
      DNS server IP ............................. 0.0.0.0

Client Dhcp Required:     False
Allowed (URL)IP Addresses
-------------------------
209.165.200.225
209.165.200.226
209.165.200.227
209.165.200.228
209.165.200.229
209.165.200.230
209.165.200.231
209.165.200.232
209.165.200.233
209.165.200.234
209.165.200.235
209.165.200.236
209.165.200.237
209.165.200.238
209.165.201.1
209.165.201.2
209.165.201.3
209.165.201.4
209.165.201.5
209.165.201.6
209.165.201.7
209.165.201.8
209.165.201.9
209.165.201.10
```

show client location-calibration summary

クライアントのロケーション調整要約情報を表示するには、**show client location-calibration summary** コマンドを使用します。

show client location-calibration summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ロケーション調整要約情報を表示する例を示します。

```
(Cisco Controller) >show client location-calibration summary
MAC Address Interval
----------- ----------
10:10:10:10:10:10 60
21:21:21:21:21:21 45
```

show client roam-history

指定されたクライアントのローミング履歴を表示するには、**show client roam-history** コマンドを使用します。

show client roam-history *mac_address*

構文の説明

mac_address	クライアント MAC アドレス

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client roam-history** コマンドの出力例を示します。

```
(Cisco Controller) > show client roam-history 00:14:6c:0a:57:77
```

show client summary

Cisco Lightweight アクセス ポイントにアソシエートされているクライアントの要約を表示するには、**show client summary** コマンドを使用します。

show client summary [*ssid / ip / username / devicetype*]

構文の説明

、このコマンドには引数またはキーワードはありません。

構文の説明

ssid / ip / username / devicetype	（任意）次のパラメータのいずれか、または任意の順序のすべてのパラメータで、アクティブなクライアントの選択的詳細を表示します。 • SSID • IP アドレス • ユーザ名 • デバイス タイプ（Samsung デバイスや Windows XP ワークステーションなど）

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

show client ap コマンドを使用して、自動的に無効にされたクライアントのステータスを一覧表示します。**show exclusionlist** コマンドを使用して、除外リスト（ブラックリスト）上のクライアントを表示します。

次に、アクティブなクライアントの要約を表示する例を示します。

```
(Cisco Controller) > show client summary
Number of Clients.............................. 24
Number of PMIPV6 Clients....................... 200
MAC Address       AP Name           Status        WLAN/GLAN/RLAN Auth Protocol
Port Wired  PMIPV6
----------------- ----------------- ------------- -------------- ---- ----------------
---- -----  ------

00:00:15:01:00:01 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a
13   No      Yes
00:00:15:01:00:02 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a
13   No      No
00:00:15:01:00:03 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a
13   No      Yes
00:00:15:01:00:04 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a
13   No      No
```

次に、デバイス タイプが Windows XP ワークステーションのすべてのクライアントを表示する例を示します。

```
(Cisco Controller) >show client summary WindowsXP-Workstation
Number of Clients in WLAN.......................... 0

MAC Address       AP Name    Status        Auth Protocol         Port Wired Mobility
Role

----------------- -------- ------------- ----------------      ---------- --------------

Number of Clients with requested device type..... 0
```

show client summary guest-lan

アクティブな有線ゲスト LAN クライアントを表示するには、**show client summary guest-lan** コマンドを使用します。

show client summary guest-lan

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client summary guest-lan** コマンドの出力例を示します。

```
(Cisco Controller) > show client summary guest-lan
Number of Clients.............................. 1
MAC Address       AP Name      Status         WLAN  Auth   Protocol  Port Wired
-----------       ---------    ----------     ----  ----   --------  ---- -----
00:16:36:40:ac:58  N/A         Associated        1    No      802.3     1   Yes
```

関連コマンド

show client summary

show client tsm

クライアントのトラフィック ストリーム メトリック（TSM）統計情報を表示するには、**show client tsm** コマンドを使用します。

show client tsm 802.11{**a** | **b**} *client_mac* {*ap_mac* | **all**}

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b/g ネットワークを指定します。
client_mac	クライアントの MAC アドレス。
ap_mac	TSM アクセス ポイントの MAC アドレス。
all	クライアントに関連するすべてのアクセス ポイントのリストを指定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client tsm 802.11a** コマンドの出力例を示します。

```
(Cisco Controller) > show client tsm 802.11a xx:xx:xx:xx:xx:xx all
AP Interface MAC: 00:0b:85:01:02:03
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds
  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec)..............................10
      Maximum Lost Packet count(5sec).............................5
      Average Lost Packet count(5secs)............................2
    DownLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec)..............................10
      Maximum Lost Packet count(5sec).............................5
      Average Lost Packet count(5secs)............................2
```

関連コマンド

show client ap

show client detail

show client summary

show client username

ユーザ名ごとにクライアント データを表示するには、**show client username** コマンドを使用します。

show client username *username*

構文の説明

username	クライアントのユーザ名。 コントローラのアクセス ポイントに関連付けられている、実行状態の最初の 8 つのクライアントのリストを表示することができます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client username** コマンドの出力例を示します。

```
(Cisco Controller) > show client username local

MAC Address        AP Name            Status         WLAN  Auth  Protocol          Port
  Device Type
-----------------  -----------------  -------------  ----  ----  ----------------  ----
  -----------

12:22:64:64:00:01  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
  Unknown
12:22:64:64:00:02  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
  Unknown
12:22:64:64:00:03  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
  Unknown
12:22:64:64:00:04  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
  Unknown
12:22:64:64:00:05  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
  Unknown
12:22:64:64:00:06  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
  Unknown
12:22:64:64:00:07  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
  Unknown
12:22:64:64:00:08  WEB-AUTH-AP-1      Associated     1     Yes   802.11g            1
  Unknown
```

show client voice-diag

音声診断統計情報を表示するには、**show client voice-diag** コマンドを使用します。

show client voice-diag {**quos-map** | **roam-history** | **rssi** | **status** | **tspec**}

構文の説明

quos-map	QoS/DSCP マッピングに関する情報と 4 つのキュー（VO、VI、BE、BK）それぞれのパケット統計が表示されます。各種 DSCP 値も表示されます。
roam-history	過去 3 回のローミングの履歴に関する情報が表示されます。出力には、タイムスタンプ、ローミングに関連したアクセス ポイント、およびローミングの理由が含まれ、ローミングに失敗した場合にはその理由も含まれます。
rssi	音声診断がイネーブル場合に、直前の 5 秒間のクライアントの RSSI 値を表示します。
status	クライアントの音声診断の状態を表示します。
tspec	音声診断のクライアントに対する TSPEC を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client voice-diag status** コマンドの出力例を示します。

```
(Cisco Controller) > show client voice-diag status
Voice Diagnostics Status: FALSE
```

関連コマンド

show client ap

show client detail

show client summary

debug voice-diag

show client detail

Cisco Lightweight アクセス ポイント上のクライアントの詳細情報を表示するには、**show client detail** コマンドを使用します。

show client detail *mac_address*

構文の説明

mac_address	クライアント MAC アドレス

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

show client ap コマンドは自動的に無効にされたクライアントのステータスを表示できます。**show exclusionlist** コマンドを使用して、除外リスト（ブラックリスト）上のクライアントを表示します。

次に、クライアントの詳細情報を表示する例を示します。

```
(Cisco Controller) >show client detail 00:0c:41:07:33:a6
Policy Manager State.............................POSTURE_REQD
Policy Manager Rule Created.....................Yes
Client MAC Address.............................. 00:16:36:40:ac:58
Client Username.................................. N/A
Client State..................................... Associated
Client NAC OOB State............................. QUARANTINE
Guest LAN Id..................................... 1
IP Address....................................... Unknown
Session Timeout.................................. 0
QoS Level........................................ Platinum
802.1P Priority Tag.............................. disabled
KTS CAC Capability............................... Yes
WMM Support...................................... Enabled
Power Save....................................... ON
Diff Serv Code Point (DSPC)...................... disabled
Mobility State................................... Local
Internal Mobility State.......................... apfMsMmInitial
Security Policy Completed........................ No
Policy Manager State............................. WEBAUTH_REQD
Policy Manager Rule Created...................... Yes
NPU Fast Fast Notified........................... Yes
Last Policy Manager State........................ WEBAUTH_REQD
Client Entry Create Time......................... 460 seconds
Interface........................................ wired-guest
FlexConnect Authentication....................... Local
FlexConnect Data Switching....................... Local
VLAN............................................. 236
Quarantine VLAN.................................. 0
Client Statistics:
  Number of Bytes Received................... 66806
      Number of Data Bytes Received.................... 160783
      Number of Realtime Bytes Received................ 160783
      Number of Data Bytes Sent....................... 23436
```

```
        Number of Realtime Bytes Sent..................... 23436
        Number of Data Packets Received................... 592
        Number of Realtime Packets Received.............. 592
        Number of Data Packets Sent...................... 131
        Number of Realtime Packets Sent.................. 131
        Number of Interim-Update Sent..............  0
        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.....................  0
        Number of RTS Retries......................  0
        Number of Duplicate Received Packets.......  3
        Number of Decrypt Failed Packets...........  0
        Number of Mic Failured Packets.............  0
        Number of Mic Missing Packets..............  0
    Number of RA Packets Dropped.............. 6
        Number of Policy Errors....................  0
        Radio Signal Strength Indicator.............  -50 dBm
        Signal to Noise Ratio......................  43 dB
...
```

show client location-calibration summary

クライアントのロケーション調整要約情報を表示するには、**show client location-calibration summary** コマンドを使用します。

show client location-calibration summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ロケーション調整要約情報を表示する例を示します。

```
(Cisco Controller) >show client location-calibration summary
MAC Address Interval
----------- ----------
10:10:10:10:10:10 60
21:21:21:21:21:21 45
```

show client probing

プローブ クライアントの数を表示するには、**show client probing** コマンドを使用します。

show client probing

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、プローブ クライアントの数を表示する例を示します。

```
(Cisco Controller) >show client probing
Number of Probing Clients..................... 0
```

show client roam-history

指定されたクライアントのローミング履歴を表示するには、**show client roam-history** コマンドを使用します。

show client roam-history *mac_address*

構文の説明

mac_address	クライアント MAC アドレス

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client roam-history** コマンドの出力例を示します。

```
(Cisco Controller) > show client roam-history 00:14:6c:0a:57:77
```

show client summary

Cisco Lightweight アクセス ポイントにアソシエートされているクライアントの要約を表示するには、**show client summary** コマンドを使用します。

show client summary [*ssid / ip / username / devicetype*]

構文の説明

、このコマンドには引数またはキーワードはありません。

構文の説明

ssid / ip / username / devicetype	（任意）次のパラメータのいずれか、または任意の順序のすべてのパラメータで、アクティブなクライアントの選択的詳細を表示します。 • SSID • IP アドレス • ユーザ名 • デバイス タイプ（Samsung デバイスや Windows XP ワークステーションなど）

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

show client ap コマンドを使用して、自動的に無効にされたクライアントのステータスを一覧表示します。**show exclusionlist** コマンドを使用して、除外リスト（ブラックリスト）上のクライアントを表示します。

次に、アクティブなクライアントの要約を表示する例を示します。

```
(Cisco Controller) > show client summary
Number of Clients.............................. 24
Number of PMIPV6 Clients....................... 200
MAC Address       AP Name           Status        WLAN/GLAN/RLAN Auth Protocol
Port Wired  PMIPV6
----------------- ----------------- ------------- -------------- ---- ----------------
---- -----  ------

00:00:15:01:00:01 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a
13   No      Yes
00:00:15:01:00:02 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a
13   No      No
00:00:15:01:00:03 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a
13   No      Yes
00:00:15:01:00:04 NMSP-TalwarSIM1-2 Associated    1              Yes  802.11a
13   No      No
```

次に、デバイス タイプが Windows XP ワークステーションのすべてのクライアントを表示する例を示します。

```
(Cisco Controller) >show client summary WindowsXP-Workstation
Number of Clients in WLAN.......................... 0

MAC Address       AP Name    Status        Auth Protocol         Port Wired Mobility
Role

----------------- -------- ------------- ----------------      ---------- --------------

Number of Clients with requested device type..... 0
```

show client wlan

WLAN に関連付けられているクライアントの要約を表示するには、**show client wlan** コマンドを使用します。

show client wlan *wlan_id* [**devicetype** *device*]

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
devicetype	（任意）指定したデバイス タイプのすべてのクライアントを表示します。
device	デバイス タイプ。たとえば、Samsung デバイスや Windows XP ワークステーションです。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show client wlan** コマンドの出力例を示します。

```
(Cisco Controller) > show client wlan 1

Number of Clients in WLAN..................... 0


(Cisco Controller) > show client devicetype WindowsXP-Workstation

Number of Clients in WLAN..................... 0

MAC Address       AP Name    Status        Auth Protocol         Port Wired Mobility
Role

----------------- -------- ------------ ----------------       ---------- --------------

Number of Clients with requested device type..... 0
```

show cloud-services cmx summary

CMX クラウド サービスの要約を表示するには、**show cloud-services cmx summary** コマンドを使用します。

show cloud-services cmx summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.3	このコマンドが導入されました。

次に、CMX クラウド サービスの概要の例を示します。

```
(Cisco Controller) >show cloud-services cmx summary
```

show cloud-services cmx statistics

CMX クラウド サービスの統計情報を表示するには、**show cloud-services cmx statistics** コマンドを使用します。

show cloud-services cmx statistics

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.3	このコマンドが導入されました。

次に、CMX クラウド サービスの統計情報の例を示します。

```
(Cisco Controller) >show cloud-services cmx statistics
```

show coredump summary

コントローラのコア ダンプの要約を表示するには、**show coredump summary** コマンドを使用します。

show coredump summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show coredump summary** コマンドの出力例を示します。

```
(Cisco Controller) > show coredump summary
Core Dump is enabled
FTP Server IP..................................... 10.10.10.17
FTP Filename...................................... file1
FTP Username...................................... ftpuser
FTP Password...................................... *********
```

関連コマンド

config coredump

config coredump ftp

config coredump username

show country

設定されている国とサポートされている無線タイプを表示するには、**show country** コマンドを使用します。

show country

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、設定されている国とサポートされている無線タイプを表示する例を示します。

```
(Cisco Controller) >show country
Configured Country..............................  United States
Configured Country Codes
US  - United States.............................  802.11a / 802.11b / 802.11g
```

show country channels

設定されている国でサポートされている無線タイプを表示するには、**show country channels** コマンドを使用します。

show country channels

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、設定されている国の自動 RF チャネルを表示する例を示します。

```
(Cisco Controller) >show country channels
Configured Country..............................  United States
      KEY: * = Channel is legal in this country and may be configured manually.
Configured Country..............................  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.
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG :
Channels :                   1 1 1 1 1
         : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
     US  : A * * * * A * * * * A . . .
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 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
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
     US  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

show country supported

サポートされている国のオプションのリストを表示するには、**show country supported** コマンドを使用します。

show country supported

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、すべてのサポート対象国リストを表示する例を示します。

```
(Cisco Controller) >show country supported
Configured Country............................ United States
Supported Country Codes
AR  - Argentina.............................. 802.11a / 802.11b / 802.11g
AT  - Austria................................ 802.11a / 802.11b / 802.11g
AU  - Australia.............................. 802.11a / 802.11b / 802.11g
BR  - Brazil................................. 802.11a / 802.11b / 802.11g
BE  - Belgium................................ 802.11a / 802.11b / 802.11g
BG  - Bulgaria............................... 802.11a / 802.11b / 802.11g
CA  - Canada................................. 802.11a / 802.11b / 802.11g
CH  - Switzerland............................ 802.11a / 802.11b / 802.11g
CL  - Chile..................................           802.11b / 802.11g
CN  - China.................................. 802.11a / 802.11b / 802.11g
CO  - Colombia...............................           802.11b / 802.11g
CY  - Cyprus................................. 802.11a / 802.11b / 802.11g
CZ  - Czech Republic......................... 802.11a / 802.11b
DE  - Germany................................ 802.11a / 802.11b / 802.11g
DK  - Denmark................................ 802.11a / 802.11b / 802.11g
EE  - Estonia................................ 802.11a / 802.11b / 802.11g
ES  - Spain.................................. 802.11a / 802.11b / 802.11g
FI  - Finland................................ 802.11a / 802.11b / 802.11g
FR  - France................................. 802.11a / 802.11b / 802.11g
GB  - United Kingdom......................... 802.11a / 802.11b / 802.11g
GI  - Gibraltar.............................. 802.11a / 802.11b / 802.11g
GR  - Greece................................. 802.11a / 802.11b / 802.11g
HK  - Hong Kong.............................. 802.11a / 802.11b / 802.11g
HU  - Hungary................................ 802.11a / 802.11b / 802.11g
ID  - Indonesia..............................           802.11b / 802.11g
IE  - Ireland................................ 802.11a / 802.11b / 802.11g
IN  - India.................................. 802.11a / 802.11b / 802.11g
IL  - Israel................................. 802.11a / 802.11b / 802.11g
ILO - Israel (outdoor)......................           802.11b / 802.11g
IS  - Iceland................................ 802.11a / 802.11b / 802.11g
IT  - Italy.................................. 802.11a / 802.11b / 802.11g
JP  - Japan (J).............................. 802.11a / 802.11b / 802.11g
J2  - Japan 2(P)............................. 802.11a / 802.11b / 802.11g
J3  - Japan 3(U)............................. 802.11a / 802.11b / 802.11g
KR  - Korea Republic (C)..................... 802.11a / 802.11b / 802.11g
KE  - Korea Extended (K)..................... 802.11a / 802.11b / 802.11g
LI  - Liechtenstein.......................... 802.11a / 802.11b / 802.11g
LT  - Lithuania.............................. 802.11a / 802.11b / 802.11g
LU  - Luxembourg............................. 802.11a / 802.11b / 802.11g
LV  - Latvia................................. 802.11a / 802.11b / 802.11g
MC  - Monaco................................. 802.11a / 802.11b / 802.11g
MT  - Malta.................................. 802.11a / 802.11b / 802.11g
```

```
MX  - Mexico..................................... 802.11a / 802.11b / 802.11g
MY  - Malaysia................................... 802.11a / 802.11b / 802.11g
NL  - Netherlands................................ 802.11a / 802.11b / 802.11g
NZ  - New Zealand................................ 802.11a / 802.11b / 802.11g
NO  - Norway..................................... 802.11a / 802.11b / 802.11g
PA  - Panama.....................................           802.11b / 802.11g
PE  - Peru.......................................           802.11b / 802.11g
PH  - Philippines................................ 802.11a / 802.11b / 802.11g
PL  - Poland..................................... 802.11a / 802.11b / 802.11g
PT  - Portugal................................... 802.11a / 802.11b / 802.11g
RU  - Russian Federation......................... 802.11a / 802.11b / 802.11g
RO  - Romania.................................... 802.11a / 802.11b / 802.11g
SA  - Saudi Arabia............................... 802.11a / 802.11b / 802.11g
SE  - Sweden..................................... 802.11a / 802.11b / 802.11g
SG  - Singapore.................................. 802.11a / 802.11b / 802.11g
SI  - Slovenia................................... 802.11a / 802.11b / 802.11g
SK  - Slovak Republic............................ 802.11a / 802.11b / 802.11g
TH  - Thailand...................................           802.11b / 802.11g
TR  - Turkey.....................................           802.11b / 802.11g
TW  - Taiwan..................................... 802.11a / 802.11b / 802.11g
UA  - Ukraine.................................... 802.11a / 802.11b / 802.11g
US  - United States.............................. 802.11a / 802.11b / 802.11g
USL - United States (Legacy)..................... 802.11a / 802.11b / 802.11g
USX - United States (US + chan165)............... 802.11a / 802.11b / 802.11g
VE  - Venezuela..................................           802.11b / 802.11g
ZA  - South Africa............................... 802.11a / 802.11b / 802.11g
```

show cpu

現在の WLAN コントローラの CPU 利用率情報を表示するには、**show cpu** コマンドを使用します。

show cpu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show cpu** コマンドの出力例を示します。

```
(Cisco Controller) > show cpu
Current CPU load: 2.50%
```

show custom-web

すべての Web 認証カスタマイズ情報を表示するには、**show custom-web** コマンドを使用します。

show custom-web *all remote-lan guest-lan sleep-client webauth-bundle wlan*

構文の説明

all	すべての Web 認証のカスタマイズ情報を表示します。
remote-lan	WLAN ごとの Web 認証のカスタマイズ情報を表示します。
guest-lan	ゲスト LAN ごとの Web 認証のカスタマイズ情報を表示します。
sleep-client	すべての Web 認証のスリープ状態のクライアント エントリのサマリーを表示します。
webauth-bundle	Web 認証バンドルの内容を表示します。
wlan	WLAN ごとの Web 認証のカスタマイズ情報を表示します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、7.6 以前のリリースで導入されました。
8.2	このコマンドが変更され、すべて、リモート LAN、ゲスト LAN、スリープ クライアント、web 認証バンドル、および WLAN のキーワードが追加されました。

次に、**show custom-web all** コマンドの出力例を示します。

```
(Cisco Controller) > show custom-web all
Radius Authentication Method..................... PAP
Cisco Logo....................................... Enabled
CustomLogo....................................... None
Custom Title..................................... None
Custom Message................................... None
Custom Redirect URL.............................. None
Web Authentication Type.......................... Internal Default
Logout-popup..................................... Enabled
External Web Authentication URL.................. None
```

show database summary

データベースの最大エントリ数を表示するには、**show database summary** コマンドを使用します。

show database summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、**show database summary** コマンドの出力例を示します。

```
(Cisco Controller) > show database summary
Maximum Database Entries..................... 2048
Maximum Database Entries On Next Reboot...... 2048
Database Contents
    MAC Filter Entries....................... 2
    Exclusion List Entries................... 0
    AP Authorization List Entries............ 1
    Management Users......................... 1
    Local Network Users...................... 1
        Local Users.......................... 1
        Guest Users.......................... 0
    Total................................... 5
```

関連コマンド

config database size

show dhcp

内部 Dynamic Host Configuration Protocol（DHCP）サーバ設定を表示するには、**show dhcp** コマンドを使用します。

show dhcp {**leases** | **summary** | *scope*}

構文の説明

leases	割り当てられた DHCP リースを表示します。
summary	DHCP 要約情報を表示します。
scope	そのスコープの DHCP 情報を表示するスコープの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、割り当てられた DHCP リースを表示する例を示します。

```
(Cisco Controller) >show dhcp leases
No leases allocated.
```

次に、DHCP 要約情報を表示する例を示します。

```
(Cisco Controller) >show dhcp summary
Scope Name           Enabled           Address Range
003                    No            0.0.0.0 -> 0.0.0.0
```

次に、スコープ 003 の DHCP 情報を表示する例を示します。

```
(Cisco Controller) >show dhcp 003
Enabled..................................... No
Lease Time.................................. 0
Pool Start.................................. 0.0.0.0
Pool End.................................... 0.0.0.0
Network..................................... 0.0.0.0
Netmask..................................... 0.0.0.0
Default Routers............................. 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain..................................
DNS......................................... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers........................ 0.0.0.0 0.0.0.0 0.0.0.0
```

show dhcp proxy

DHCP プロキシ処理のステータスを表示するには、**show dhcp proxy** コマンドを使用します。

show dhcp proxy

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、DHCP プロキシ情報のステータスを表示する例を示します。

```
(Cisco Controller) >show dhcp proxy

DHCP Proxy Behavior: enabled
```

show dhcp timeout

DHCP タイムアウト値を表示するには、**show dhcp timeout** コマンドを使用します。

show dhcp timeout

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、DHCP タイムアウト値を表示する例を示します。

```
(Cisco Controller) >show dhcp timeout

DHCP Timeout (seconds)..... 10
```

show dtls connections

Datagram Transport Layer Security（DTLS）サーバのステータスを表示するには、**show dtls connections** コマンドを使用します。

show dtls connections

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show dtls connections** コマンドの出力例を示します。

```
Device > show dtls connections

AP Name          Local Port    Peer IP          Peer Port     Ciphersuite
---------------- ------------- ---------------- ------------- -----------------------
1130             Capwap_Ctrl   1.100.163.210    23678         TLS_RSA _WITH_AES_128_CBC_SHA
1130             Capwap_Data   1.100.163.210    23678         TLS_RSA _WITH_AES_128_CBC_SHA
1240             Capwap_Ctrl   1.100.163.209    59674         TLS_RSA _WITH_AES_128_CBC_SHA
```

show exclusionlist

この Cisco Wireless LAN Controller にアソシエートされている、手動除外リスト（ブラックリスト）上のすべてのクライアントの要約を表示するには、**show exclusionlist** コマンドを使用します。

show exclusionlist

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、手動で除外されたすべての MAC アドレスを表示します。

次に、除外リストを表示する例を示します。

```
(Cisco Controller) > show exclusionlist
No manually disabled clients.
Dynamically Disabled Clients
-----------------------------
  MAC Address             Exclusion Reason        Time Remaining (in secs)
  -----------             ----------------        ------------------------
00:40:96:b4:82:55         802.1X Failure           51
```

関連コマンド

config exclusionlist

show flexconnect acl detailed

FlexConnectアクセス コントロール リストの詳細なサマリーを表示するには、**show flexconnect acl detailed** コマンドを使用します。

show flexconnect acl detailed *acl-name*

構文の説明

acl-name	アクセス コントロール リストの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect の詳細 ACL を表示する例を示します。

```
(Cisco Controller) >show flexconnect acl detailed acl-2
```

show flexconnect acl summary

FlexConnect のアクセス ポイントのすべてのアクセス コントロール リストのサマリーを表示するには、**show flexconnect acl summary** コマンドを使用します。

show flexconnect acl summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect ACL のサマリーを表示する例を示します。

```
(Cisco Controller) >show flexconnect acl summary
ACL Name                          Status
-------------------------------- -------
acl1                             Modified
acl10                            Modified
acl100                           Modified
acl101                           Modified
acl102                           Modified
acl103                           Modified
acl104                           Modified
acl105                           Modified
acl106                           Modified
```

show flexconnect group detail

FlexConnect グループの詳細を表示するには、**show flexconnect group detail** コマンドを使用します。

show flexconnect group detail *group_name* ［**module-vlan** | **aps**］

構文の説明

group_name	FlexConnect グループの名前。
module-vlan	グループ内の FlexConnect ローカル スイッチングのステータスと VLAN ID を表示します。
aps	FlexConnect グループの一部である AP のリストを表示します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.1	**module-vlan** および **aps** パラメータが追加されました。

次に、特定の FlexConnect グループに関する詳細情報を表示する例を示します。

```
(Cisco Controller) >show flexconnect group detail myflexgroup
Number of Ap's in Group:  1
00:0a:b8:3b:0b:c2   AP1200    Joined
Group Radius Auth Servers:
 Primary Server Index ..................... Disabled
 Secondary Server Index ................... Disabled
```

show flexconnect group summary

FlexConnect グループの最新のリストを表示するには、**show flexconnect group summary** コマンドを使用します。

show flexconnect group summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect グループの最新のリストを表示する例を示します。

```
(Cisco Controller) >show flexconnect group summary
flexconnect Group Summary:  Count 1
Group Name        # APs
Group 1       1
```

show flexconnect office-extend

FlexConnect モードの OfficeExtend アクセス ポイントに関する情報を表示するには、**show flexconnect office-extend** コマンドを使用します。

show flexconnect office-extend {**summary** | **latency**}

構文の説明

summary	すべての OfficeExtend アクセス ポイントのリストを表示します。
latency	OfficeExtend アクセス ポイントのリンク遅延を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FlexConnect officeExtend アクセス ポイントのリストに関する情報を表示する例を示します。

```
(Cisco Controller) >show flexconnect office-extend summary
Summary of OfficeExtend AP
AP Name            Ethernet MAC       Encryption  Join-Mode   Join-Time
------------------ -----------------  ----------  ----------- ----------
AP1130             00:22:90:e3:37:70   Enabled    Latency     Sun Jan 4 21:46:07 2009
AP1140             01:40:91:b5:31:70   Enabled    Latency     Sat Jan 3 19:30:25 2009
```

次に、FlexConnect officeExtend アクセス ポイントのリンク遅延を表示する例を示します。

```
(Cisco Controller) >show flexconnect office-extend latency
Summary of OfficeExtend AP link latency
AP Name              Status  Current   Maximum   Minimum
-------------------------------------------------------------------------
AP1130               Enabled 15 ms      45 ms     12 ms
AP1140               Enabled 14 ms     179 ms     12 ms
```

show flow exporter

フロー エクスポータの詳細または統計情報を表示するには、**show flow exporter** コマンドを使用します。

show flow exporter {**summary** | **statistics**}

構文の説明

summary	フロー エクスポータの要約を表示します。
statistics	送信されたレコード数や最後のレコードの送信時間など、フローエクスポータの統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show flow exporter summary** コマンドの出力例を示します。

```
(Cisco Controller) > show flow exporter summary
 Exporter-Name            Exporter-IP     Port
  =============            ============     =====
  expo1                    9.9.120.115       800
```

show flow monitor summary

NetFlow モニタの詳細を表示するには、**show flow monitor summary** コマンドを使用します。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

NetFlow レコードのモニタリングおよびエクスポートは NMS または Netflow 分析ツールとの統合に使用されます。

次に、**show flow monitor summary** の出力例を示します。

```
(Cisco Controller) > show flow monitor summary
Monitor-Name             Exporter-Name            Exporter-IP      Port  Record Name
============             =============            ===========      ====  ===========
 mon1                     expo1                   9.9.120.115     800
ipv4_client_app_flow_record
```

show guest-lan

特定の有線ゲスト LAN の設定を表示するには、**show guest-lan** コマンドを使用します。

show guest-lan *guest_lan_id*

構文の説明

guest_lan_id	選択した有線ゲスト LAN の ID。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラに設定されているすべての有線ゲスト LAN を表示するには、**show guest-lan summary** コマンドを使用します。

次に、**show guest-lan** *guest_lan_id* コマンドの出力例を示します。

```
(Cisco Controller) >show guest-lan 2
Guest LAN Identifier..................................... 1
Profile Name............................................. guestlan
Network Name (SSID)...................................... guestlan
Status................................................... Enabled
AAA Policy Override...................................... Disabled
Number of Active Clients................................. 1
Exclusionlist Timeout.................................... 60 seconds
Session Timeout.......................................... Infinity
Interface................................................ wired
Ingress Interface........................................ wired-guest
WLAN ACL................................................. unconfigured
DHCP Server.............................................. 10.20.236.90
DHCP Address Assignment Required......................... Disabled
Quality of Service....................................... Silver (best effort)
Security
 Web Based Authentication................................ Enabled
 ACL..................................................... Unconfigured
 Web-Passthrough......................................... Disabled
 Conditional Web Redirect................................ Disabled
 Auto Anchor............................................. Disabled
Mobility Anchor List
GLAN ID IP Address Status
```

show icons summary

システムのフラッシュ メモリに存在するアイコンの概要を表示するには、**show icons summary** コマンドを使用します。

show icons summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、**show icons summary** コマンドの出力例を示します。

```
Cisco Controller > show icons summary

 Icon files (downloaded) in Flash memory
  No.   Filename                  Size
  ---  ----------------------    -----
    1.  dhk_icon.png                 120694
    2.  myIconCopy1.png              120694
    3.  myIconCopy2.png              120694
```

show ike

アクティブなインターネット キー交換（IKE）セキュリティ アソシエーション（SA）を表示するには、**show ike** コマンドを使用します。

show ike {**brief** | **detailed**} *IP_or_MAC_address*

構文の説明

brief	すべてのアクティブな IKE SA の簡単なサマリーを表示します。
detailed	すべてのアクティブな IKE SA の詳細なサマリーを表示します。
IP_or_MAC_address	アクティブな IKE SA の IP または MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクティブなインターネット キー交換セキュリティ アソシエーションを表示する例を示します。

```
(Cisco Controller) > show ike brief 209.165.200.254
```

show interface summary

システム インターフェイスのサマリー詳細を表示するには、**show interface summary** コマンドを使用します。

show interface summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは更新され、IPv6 関連の詳細を表示するようになりました。

次に、ローカル IPv4 インターフェイスのサマリーの例を示します。

```
(Cisco Controller) > show interface summary
Number of Interfaces..... 6

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
dyn59                            LAG  59       9.10.59.66      Dynamic No     No
management                       LAG  56       9.10.56.60      Static  Yes    No
redundancy-management            LAG  56       0.0.0.0         Static  No     No
redundancy-port                  -    untagged 0.0.0.0         Static  No     No
service-port                     N/A  N/A      2.2.2.2         Static  No     No
virtual                          N/A  N/A      1.2.3.4         Static  No     No
```

次に、ローカル IPv6 インターフェイスのサマリーの例を示します。

```
show ipv6 interface summary
Number of Interfaces..... 2

Interface Name          Port Vlan Id  IPv6 Address/Prefix Length
----------------------- ---- -------- -----------------------------------------
management              LAG  56                    fe80::224:97ff:fe69:69af/64
                        LAG  56                       2001:9:10:56::60/64
service-port            N/A  N/A                   fe80::224:97ff:fe69:69a1/64
                        N/A  N/A                                      ::/128
```

show interface detailed

システム インターフェイスの詳細を表示するには、**show interface** コマンドを使用します。

show interfacedetailed {*interface_name* | **management** | **redundancy-management** | **redundancy-port** | **service-port** | **virtual**}

構文の説明

detailed	詳細なインターフェイス情報を表示します。
interface_name	詳細表示のインターフェイス名。
management	詳細な管理インターフェイス情報を表示します。
redundancy-management	詳細な冗長管理インターフェイス情報を表示します。
redundancy-port	詳細な冗長ポート情報を表示します。
service-port	詳細なサービス ポート情報を表示します。
virtual	詳細な仮想ゲートウェイ インターフェイス情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。
8.0	このコマンドはリリース8.0で更新され、IPv6関連の詳細を表示するようになりました。

次に、詳細なインターフェイス情報を表示する例を示します。

```
(Cisco Controller) > show interface detailed management

Interface Name................................. management
MAC Address.................................... 00:24:97:69:69:af
IP Address..................................... 9.10.56.60
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 9.10.56.1
External NAT IP State.......................... Disabled
External NAT IP Address........................ 0.0.0.0
Link Local IPv6 Address........................ fe80::224:97ff:fe69:69af/64
STATE ......................................... REACHABLE
Primary IPv6 Address........................... 2001:9:10:56::60/64
STATE ......................................... REACHABLE
Primary IPv6 Gateway........................... fe80::aea0:16ff:fe4f:2242
Primary IPv6 Gateway Mac Address............... ac:a0:16:4f:22:42
```

```
STATE ..................................... REACHABLE
VLAN....................................... 56
Quarantine-vlan............................ 0
NAS-Identifier............................. Building1
Active Physical Port....................... LAG (13)
Primary Physical Port...................... LAG (13)
Backup Physical Port....................... Unconfigured
DHCP Proxy Mode............................ Global
Primary DHCP Server........................ 9.1.0.100
Secondary DHCP Server...................... Unconfigured
DHCP Option 82............................. Disabled
DHCP Option 82 bridge mode insertion....... Disabled
IPv4 ACL................................... Unconfigured
IPv6 ACL................................... Unconfigured
mDNS Profile Name.......................... Unconfigured
AP Manager................................. Yes
Guest Interface............................ No
L2 Multicast............................... Enabled
```

（注） 一部の WLAN コントローラは、物理ポートが 1 つしか表示されないことがありますが、それは物理ポートが 1 つしかないためです。

次に、詳細な冗長管理インターフェイス情報を表示する例を示します。

```
(Cisco Controller) > show interface detailed redundancy-management
Interface Name............................... redundancy-management
MAC Address.................................. 88:43:e1:7e:0b:20
IP Address................................... 209.165.201.2
```

次に、詳細な冗長ポート情報を表示する例を示します。

```
(Cisco Controller) > show interface detailed redundancy-port
Interface Name............................... redundancy-port
MAC Address.................................. 88:43:e1:7e:0b:22
IP Address................................... 169.254.120.5
```

次に、詳細なサービス ポート情報を表示する例を示します。

```
(Cisco Controller) > show interface detailed service-port
Interface Name............................... redundancy-port
MAC Address.................................. 88:43:e1:7e:0b:22
IP Address................................... 169.254.120.5
```

次に、詳細な仮想ゲートウェイ インターフェイス情報を表示する例を示します。

```
(Cisco Controller) > show interface detailed virtual
Interface Name............................... virtual
MAC Address.................................. 88:43:e1:7e:0b:20
IP Address................................... 192.0.2.1
Virtual DNS Host Name........................ Disabled
```

```
AP Manager..................................... No
Guest Interface................................ No
```

show interface group

システム インターフェイス グループの詳細を表示するには、**show interface group** コマンドを使用します。

show interface group {**summary** | **detailed** *interface_group_name*}

構文の説明

summary	ローカル インターフェイス グループの要約を表示します。
detailed	詳細なインターフェイス グループ情報を表示します。
interface_group_name	詳細表示のインターフェイス グループ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ローカル インターフェイス グループの要約を表示する例を示します。

```
(Cisco Controller) > show interface group summary
Interface Group Name    Total Interfaces   Total WLANs     Total AP
Groups     Quarantine
-------------------   ---------------   ---------     -------------      ---------
mygroup1                    1              0               0              No
mygroup2                    1              0               0              No
mygroup3                    5              1               0              No
```

次に、詳細なインターフェイス グループ情報を表示する例を示します。

```
(Cisco Controller) > show interface group detailed mygroup1
Interface Group Name............................... mygroup1
Quarantine ........................................ No
Number of Wlans using the Interface Group........ 0
Number of AP Groups using the Interface Group.... 0
Number of Interfaces Contained................... 1
mDNS Profile Name.............................. NCS12Prof
Interface Group Description...................... My Interface Group
Next interface for allocation to client.......... testabc
Interfaces Contained in this group .............. testabc
Interface marked with * indicates DHCP dirty interface
```

```
Interface list sorted based on vlan:

Index  Vlan     Interface Name
-----  ----    --------------------------------
0       42      testabc
```

show invalid-config

編集した設定ファイル内の無視されたコマンドまたは無効な設定値を確認するには、**show invalid-config** コマンドを使用します。

show invalid-config

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、**clear config** または **save config** コマンドの前にのみ入力することができます。

次に、**show invalid-config** コマンドの出力例を示します。

```
(Cisco Controller) > show invalid-config
config wlan peer-blocking drop 3
config wlan dhcp_server 3 192.168.0.44 required
```

show inventory

Cisco Wireless LAN Controller の物理的なインベントリを表示するには、**show inventory** コマンドを使用します。

show inventory

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

show IPsec

アクティブなインターネットプロトコルセキュリティ（IPSec）セキュリティアソシエーション（SA）を表示するには、**show IPsec** コマンドを使用します。

show IPsec {**brief** | **detailed**} *IP_or_MAC_address*

構文の説明

brief	アクティブな IPSec SA の簡単なサマリーを表示します。
detailed	アクティブな IPSec SA の詳細なサマリーを表示します。
IP_or_MAC_address	デバイスのIPアドレスまたはMACアドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、実行中のインターネット プロトコル セキュリティ（IPSec）セキュリティ アソシエーション（SA）に関する簡単な情報を表示する例を示します。

```
(Cisco Controller) > show IPsec brief 209.165.200.254
```

関連コマンド

config radius acct ipsec authentication

config radius acct ipsec disable

config radius acct ipsec enable

config radius acct ipsec encryption

config radius auth IPsec encryption

config radius auth IPsec authentication

config radius auth IPsec disable

config radius auth IPsec encryption

config radius auth IPsec ike

config trapflags IPsec

config wlan security IPsec disable

config wlan security IPsec enable

config wlan security IPsec authentication

config wlan security IPsec encryption

config wlan security IPsec config

config wlan security IPsec ike authentication

config wlan security IPsec ike dh-group

config wlan security IPsec ike lifetime

config wlan security IPsec ike phase1

config wlan security IPsec ike contivity

show ipv6 acl

コントローラに設定されている IPv6 アクセス コントロール リスト（ACL）を表示するには、**show ipv6 acl** コマンドを使用します。

show ipv6 acl detailed {*acl_name* | **summary**}

構文の説明

acl_name	IPv6 ACL の名前。名前には 32 文字以内の英数字を使用できます。
detailed	特定の ACL の詳細情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス コントロール リストの詳細情報を表示する例を示します。

```
(Cisco Controller) >show ipv6 acl detailed acl6
Rule Index..................................... 1
Direction...................................... Any
IPv6 source prefix............................. ::/0
IPv6 destination prefix........................ ::/0
Protocol....................................... Any
Source Port Range.............................. 0-65535
Destination Port Range......................... 0-65535
DSCP........................................... Any
Flow label..................................... 0
Action......................................... Permit
Counter........................................ 0
Deny Counter................................... 0
```

show ipv6 summary

現在の IPv6 コンフィギュレーション設定を表示するには、**show ipv6 summary** コマンドを使用します。

show ipv6 summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show ipv6 summary** コマンドの出力例を示します。

```
(Cisco Controller) >show ipv6 summary
Global Config.............................. Enabled
Reachable-lifetime value..................... 30
Stale-lifetime value......................... 300
Down-lifetime value.......................... 300
RA Throttling................................ Disabled
RA Throttling allow at-least................. 1
RA Throttling allow at-most.................. no-limit
RA Throttling max-through.................... 5
RA Throttling throttle-period................ 600
RA Throttling interval-option................ ignore
NS Mulitcast CacheMiss Forwarding............ Enabled
NA Mulitcast Forwarding...................... Enabled
IPv6 Capwap UDP Lite........................ Enabled
Operating System IPv6 state ................. Enabled
```

show guest-lan

特定の有線ゲスト LAN の設定を表示するには、**show guest-lan** コマンドを使用します。

show guest-lan *guest_lan_id*

構文の説明

guest_lan_id	選択した有線ゲスト LAN の ID。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

コントローラに設定されているすべての有線ゲスト LAN を表示するには、**show guest-lan summary** コマンドを使用します。

次に、**show guest-lan** *guest_lan_id* コマンドの出力例を示します。

```
(Cisco Controller) >show guest-lan 2
Guest LAN Identifier.......................... 1
Profile Name.................................. guestlan
Network Name (SSID)........................... guestlan
Status........................................ Enabled
AAA Policy Override........................... Disabled
Number of Active Clients...................... 1
Exclusionlist Timeout......................... 60 seconds
Session Timeout............................... Infinity
Interface..................................... wired
Ingress Interface............................. wired-guest
WLAN ACL...................................... unconfigured
DHCP Server................................... 10.20.236.90
DHCP Address Assignment Required.............. Disabled
Quality of Service............................ Silver (best effort)
Security
 Web Based Authentication.................... Enabled
 ACL.......................................... Unconfigured
 Web-Passthrough.............................. Disabled
 Conditional Web Redirect..................... Disabled
 Auto Anchor.................................. Disabled
Mobility Anchor List
GLAN ID IP Address Status
```

show icons file-info

アイコン パラメータを表示するには、**show icons file-info** コマンドを使用します。

show icons file-info

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

次に、**show icons file-info** コマンドの出力例を示します。

```
Cisco Controller > show icons file-info

ICON File Info:
  No.   Filename                      Type         Lang  Width  Height
  ----  ------------------------      ------       ----  -----  ------
   1    dhk_icon.png                  png          eng   200    300
   2    myIconCopy2.png               png          eng   222    333
   3    myIconCopy1.png               png          eng   555    444
```

show ipv6 acl

コントローラに設定されている IPv6 アクセス コントロール リスト（ACL）を表示するには、**show ipv6 acl** コマンドを使用します。

show ipv6 acl detailed {*acl_name* | **summary**}

構文の説明

acl_name	IPv6 ACL の名前。名前には 32 文字以内の英数字を使用できます。
detailed	特定の ACL の詳細情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス コントロール リストの詳細情報を表示する例を示します。

```
(Cisco Controller) >show ipv6 acl detailed acl6
Rule Index..................................... 1
Direction...................................... Any
IPv6 source prefix............................. ::/0
IPv6 destination prefix........................ ::/0
Protocol....................................... Any
Source Port Range.............................. 0-65535
Destination Port Range......................... 0-65535
DSCP........................................... Any
Flow label..................................... 0
Action......................................... Permit
Counter........................................ 0
Deny Counter................................... 0
```

show ipv6 acl cpu

IPv6 ACL の CPU 詳細を表示するには、**show ipv6 acl cpu** コマンドを使用します。

show ipv6 acl cpu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは IPv6 アドレス形式をサポートします。

次に、**show ipv6 acl cpu** コマンドの出力例を示します。

```
(Cisco Controller) > show ipv6 acl cpu

CPU Acl Name.............................. NOT CONFIGURED
Wireless Traffic.......................... Disabled
Wired Traffic............................. Disabled
```

show ipv6 acl detailed

IPv6 ACL の詳細を表示するには、**show ipv6 acl detailed** コマンドを使用します。

show ipv6 acl detailed

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは IPv6 アドレス形式をサポートします。

次に、**show ipv6 acl detailed TestACL** コマンドの出力例を示します。

```
(Cisco Controller) > show ipv6 acl detailed ddd

Rule Index..................................... 1
Direction...................................... Any
IPv6 source prefix............................. 2001:9:5:90::115/128
IPv6 destination prefix........................ ::/0
Protocol....................................... 6
Source Port Range.............................. 0-65535
Destination Port Range......................... 0-65535
DSCP........................................... Any
Action......................................... Permit
Counter........................................ 0

Rule Index..................................... 2
Direction...................................... Any
IPv6 source prefix............................. ::/0
IPv6 destination prefix........................ 2001:9:5:90::115/128
Protocol....................................... 6
Source Port Range.............................. 0-65535
Destination Port Range......................... 0-65535
DSCP........................................... Any
Action......................................... Permit
Counter........................................ 0
```

show ipv6 neighbor-binding

コントローラに設定された IPv6 ネイバー バインディング データを表示するには、**show ipv6 neighbor-binding** コマンドを使用します。

show ipv6 neighbor-binding {**capture-policy** | **counters** | **detailed** {**mac** *mac_address* | **port** *port_number* | **vlan***vlan_id*} | **features** | **policies** | **ra-throttle** {**statistics** *vlan_id* | **routers** *vlan_id*} | **summary**}

構文の説明

capture-policy	IPv6 ネクスト ホップ メッセージ キャプチャ ポリシーを表示します。
counters	IPv6 ネクスト ホップ カウンタを表示します（ブリッジ モードのみ）。
detailed	IPv6 ネイバー バインディング テーブルを表示します。
mac	特定の MAC アドレスの IPv6 バインディング テーブル エントリを表示します。
mac_address	特定の MAC アドレスの IPv6 バインディング テーブル エントリを表示します。
port	特定のポートの IPv6 バインディング テーブル エントリを表示します。
port_number	ポート番号。LAG ポートのアクセス ポイントまたは LAG に対して、ap を入力できます。
vlan	特定の VLAN の IPv6 ネイバー バインディング テーブル エントリを表示します。
vlan_id	VLAN 識別番号。
features	IPv6 ネクスト ホップ登録機能を表示します。
policies	IPv6 ネクスト ホップのポリシーを表示します。
ra-throttle	RA スロットル情報を表示します。
statistics	RA スロットル統計情報を表示します。
routers	RA スロットル ルータを表示します。
summary	IPv6 ネイバー バインディング テーブルを表示します。

コマンド デフォルト なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン DHCPv6 カウンタは、IPv6 ブリッジ モードにのみ適用されます。

次に、**show ipv6 neighbor-binding summary** コマンドの出力を示します。

```
(Cisco Controller) >show ipv6 neighbor-binding summary
Binding Table has 6 entries, 5 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DDCP
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted access   0010:Orig trusted trunk    0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
    IPv6 address                              MAC Address       Port VLAN Type     prlvl
 age  state     Time left
-- ----------------------------------------  ----------------- ---- ---- -------- -----
 ---- --------- ----------
ND  fe80::216:46ff:fe43:eb01                 00:16:46:43:eb:01    1  980 wired     0005
    2 REACHABLE  157
ND  fe80::9cf9:b009:b1b4:1ed9                70:f1:a1:dd:cb:d4   AP  980 wireless  0005
    2 REACHABLE  157
ND  fe80::6233:4bff:fe05:25ef                60:33:4b:05:25:ef   AP  980 wireless  0005
    2 REACHABLE  203
ND  fe80::250:56ff:fe8b:4a8f                 00:50:56:8b:4a:8f   AP  980 wireless  0005
    2 REACHABLE  157
ND  2001:410:0:1:51be:2219:56c6:a8ad         70:f1:a1:dd:cb:d4   AP  980 wireless  0005
    5 REACHABLE  157
S   2001:410:0:1::9                          00:00:00:00:00:08   AP  980 wireless  0100
    1 REACHABLE  205
```

次に、**show ipv6 neighbor-binding detailed** コマンドの出力を示します。

```
(Cisco Controller) >show ipv6 neighbor-binding detailed mac 60:33:4b:05:25:ef
macDB has 3 entries for mac 60:33:4b:05:25:ef, 3 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DDCP
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted access   0010:Orig trusted trunk    0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
    IPv6 address                              MAC Address       Port VLAN Type     prlvl
 age  state     Time left
-- ----------------------------------------  ----------------- ---- ---- -------- -----
 ---- --------- ----------
ND  fe80::6233:4bff:fe05:25ef                60:33:4b:05:25:ef   AP  980 wireless  0009
    0 REACHABLE  303
ND  2001:420:0:1:6233:4bff:fe05:25ef         60:33:4b:05:25:ef   AP  980 wireless  0009
    0 REACHABLE  300
ND  2001:410:0:1:6233:4bff:fe05:25ef         60:33:4b:05:25:ef   AP  980 wireless  0009
    0 REACHABLE  301
```

次に、**show ipv6 neighbor-binding counters** コマンドの出力を示します。

```
(Cisco Controller) >show ipv6 neighbor-binding counters
Received Messages
```

```
NDP Router Solicitation                 6
NDP Router Advertisement                19
NDP Neighbor Solicitation               557
NDP Neighbor Advertisement              48
NDP Redirect                            0
NDP Certificate Solicit                 0
NDP Certificate Advert                  0
DHCPv6 Solicitation                     0
DHCPv6 Advertisement                    0
DHCPv6 Request                          0
DHCPv6 Reply                            0
DHCPv6 Inform                           0
DHCPv6 Confirm                          0
DHCPv6 Renew                            0
DHCPv6 Rebind                           0
DHCPv6 Release                          0
DHCPv6 Decline                          0
DHCPv6 Reconfigure                      0
DHCPv6 Relay Forward                    0
DHCPv6 Relay Rep                        0

Bridged Messages

NDP Router Solicitation                 6
NDP Router Advertisement                19
NDP Neighbor Solicitation               471
NDP Neighbor Advertisement              16
NDP Redirect                            0
NDP Certificate Solicit                 0
NDP Certificate Advert                  0
DHCPv6 Solicitation                     0
DHCPv6 Advertisement                    0
DHCPv6 Request                          0
DHCPv6 Reply                            0
DHCPv6 Inform                           0
DHCPv6 Confirm                          0
DHCPv6 Renew                            0
DHCPv6 Rebind                           0
DHCPv6 Release                          0
DHCPv6 Decline                          0
DHCPv6 Reconfigure                      0
DHCPv6 Relay Forward                    0
DHCPv6 Relay Rep                        0

NDSUPRRESS Drop counters

total   silent ns_in_out ns_dad unicast multicast internal
------------------------------------------------------------------------
0       0       0       0       0       0       0

SNOOPING Drop counters

Dropped Msgs            total   silent  internal CGA_vfy  RSA_vfy  limit  martian
martian_mac  no_trust  not_auth  stop
-------------------------------------------------------------------------------------------------------
NDP RS                          0       0       0       0       0       0       0
 0       0       0       0
NDP RA                          0       0       0       0       0       0       0
 0       0       0       0
NDP NS                          0       0       0       0       0       0       0
 0       0       0       0
NDP NA                          0       0       0       0       0       0       0
 0       0       0       0
```

```
NDP Redirect                    0       0       0       0       0       0       0
 0       0       0       0
NDP CERT SOL                    0       0       0       0       0       0       0
 0       0       0       0
NDP CERT ADV                    0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Sol                      0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Adv                      0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Req                      0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Confirm                  0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Renew                    0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Rebind                   0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Reply                    0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Release                  0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Decline                  0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Recfg                    0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Infreq                   0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Relayfwd                 0       0       0       0       0       0       0
 0       0       0       0
DHCPv6 Relayreply               0       0       0       0       0       0       0
 0       0       0       0

CacheMiss Statistics
        Multicast NS Forwarded
                To STA  0
                To DS   0
        Multicast NS Dropped
                To STA  467
                To DS   467

Multicast NA Statistics
        Multicast NA Forwarded
                To STA  0
                To DS   0
        Multicast NA Dropped
                To STA  0
                To DS   0

(Cisco Controller) > >
```

show ipv6 ra-guard

RA ガードの統計情報を表示するには、**show ipv6 ra-guard** コマンドを使用します。

show ipv6 ra-guard {**ap** | **wlc**} **summary**

構文の説明

ap	Cisco アクセス ポイントの詳細を表示します。
wlc	Cisco コントローラの詳細を表示します。
summary	RA ガードの統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show ipv6 ra-guard ap summary** コマンドの出力例を示します。

```
(Cisco Controller) >show ipv6 ra-guard ap summary
IPv6 RA Guard on AP..................... Enabled
RA Dropped per client:
MAC Address       AP Name           WLAN/GLAN      Number of RA Dropped
----------------- ----------------- -------------- ---------------------
00:40:96:b9:4b:89 Bhavik_1130_1_p13 2              19
----------------- ----------------- -------------- ---------------------
Total RA Dropped on AP.....................      19
```

次に、コントローラの RA ガード統計情報を表示する例を示します。

```
(Cisco Controller) >show ipv6 ra-guard wlc summary
IPv6 RA Guard on WLC.................... Enabled
```

show ipv6 route summary

IPv6 ルートの設定情報を表示するには、**show ipv6 route summary** コマンドを使用します。

show ipv6 route summary

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

次に、**show ipv6 route summary** コマンドの出力例を示します。

```
(Cisco Controller) > show ipv6 route summary
Number of Routes.............................. 1

Destination Network PrefixLength Gateway
------------------- ------------- --------------------
2001:9:5:90::115 /128 2001:9:5:91::1
```

show ipv6 summary

現在の IPv6 コンフィギュレーション設定を表示するには、**show ipv6 summary** コマンドを使用します。

show ipv6 summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show ipv6 summary** コマンドの出力例を示します。

```
(Cisco Controller) >show ipv6 summary
Global Config.............................. Enabled
Reachable-lifetime value..................... 30
Stale-lifetime value......................... 300
Down-lifetime value.......................... 300
RA Throttling.............................. Disabled
RA Throttling allow at-least................. 1
RA Throttling allow at-most.................. no-limit
RA Throttling max-through.................... 5
RA Throttling throttle-period................ 600
RA Throttling interval-option................ ignore
NS Mulitcast CacheMiss Forwarding........... Enabled
NA Mulitcast Forwarding...................... Enabled
IPv6 Capwap UDP Lite........................ Enabled
Operating System IPv6 state ................ Enabled
```

show known ap

既知の Cisco Lightweight アクセス ポイントの情報を表示するには、**show known ap** コマンドを使用します。

show known ap {**summary** | **detailed** *MAC*}

構文の説明

summary	既知のすべてのアクセス ポイントのリストを表示します。
detailed	既知のすべてのアクセス ポイントの詳細情報を提供します。
MAC	既知の AP の MAC アドレス。

コマンド デフォルト

なし

次に、すべての既知のアクセス ポイントの要約を表示する例を示します。

```
(Cisco Controller) >show known ap summary
MAC Address         State        # APs  # Clients   Last Heard
-----------         -----------  -----   --------   -----------------
```

show コマンド：j ～ q

- show l2tp （1614 ページ）
- show lag eth-port-hash （1615 ページ）
- show lag ip-port-hash （1616 ページ）
- show lag summary （1617 ページ）
- show ldap （1618 ページ）
- show ldap statistics （1619 ページ）
- show ldap summary （1620 ページ）
- show license all （1621 ページ）
- show license capacity （1623 ページ）
- show license detail （1624 ページ）
- show license expiring （1625 ページ）
- show license evaluation （1626 ページ）
- show license feature （1627 ページ）
- show license file （1628 ページ）
- show license handle （1629 ページ）
- show license image-level （1630 ページ）
- show license in-use （1631 ページ）
- show license permanent （1632 ページ）
- show license status （1633 ページ）
- show license statistics （1634 ページ）
- show license summary （1635 ページ）
- show license udi （1637 ページ）
- show license usage （1638 ページ）
- show load-balancing （1639 ページ）
- show local-auth config （1640 ページ）
- show local-auth statistics （1642 ページ）
- show local-auth certificates （1644 ページ）
- show logging （1645 ページ）
- show logging config-history （1647 ページ）

- show logging flags （1648 ページ）
- show loginsession （1649 ページ）
- show macfilter （1650 ページ）
- show mdns ap summary （1651 ページ）
- show mdns domain-name-ip summary （1652 ページ）
- show mdns profile （1654 ページ）
- show mdns service （1656 ページ）
- show media-stream client （1658 ページ）
- show media-stream group detail （1659 ページ）
- show media-stream group summary （1660 ページ）
- show mesh ap （1661 ページ）
- show mesh astools stats （1663 ページ）
- show mesh backhaul （1664 ページ）
- show mesh cac （1665 ページ）
- show mesh client-access （1667 ページ）
- show mesh config （1668 ページ）
- show mesh convergence （1669 ページ）
- show mesh env （1670 ページ）
- show mesh neigh （1671 ページ）
- show mesh path （1674 ページ）
- show mesh per-stats （1675 ページ）
- show mesh public-safety （1676 ページ）
- show mesh queue-stats （1677 ページ）
- show mesh security-stats （1678 ページ）
- show mesh stats （1680 ページ）
- show mgmtuser （1681 ページ）
- show mobility anchor （1682 ページ）
- show mobility ap-list （1684 ページ）
- show mobility foreign-map （1685 ページ）
- show mobility group member （1686 ページ）
- show mobility oracle （1687 ページ）
- show mobility statistics （1689 ページ）
- show mobility summary （1690 ページ）
- show msglog （1692 ページ）
- show nac statistics （1693 ページ）
- show nac summary （1694 ページ）
- show network （1695 ページ）
- show network summary （1696 ページ）
- show netuser （1698 ページ）
- show netuser guest-roles （1699 ページ）
- show network multicast mgid detail （1700 ページ）

- show network multicast mgid summary （1701 ページ）
- show network summary （1702 ページ）
- show nmsp notify-interval summary （1704 ページ）
- show nmsp status （1705 ページ）
- show nmsp statistics （1706 ページ）
- show nmsp subscription （1708 ページ）
- show nmsp subscription summary （1710 ページ）
- show ntp-keys （1711 ページ）
- show ntp-keys （1712 ページ）
- show pmk-cache （1713 ページ）
- show pmipv6 domain （1714 ページ）
- show pmipv6 mag bindings （1715 ページ）
- show pmipv6 mag globals （1716 ページ）
- show pmipv6 mag stats （1717 ページ）
- show pmipv6 profile summary （1719 ページ）
- show policy （1720 ページ）
- show port （1722 ページ）
- show profiling policy summary （1724 ページ）
- show qos （1727 ページ）
- show qos qosmap （1728 ページ）
- show queue-info （1729 ページ）

show l2tp

レイヤ 2 トンネリング プロトコル（L2TP）セッションを表示するには、**show l2tp** コマンドを使用します。

show l2tp {**summary** | *ip_address* }

構文の説明

summary	すべての L2TP セッションを表示します。
ip_address	IP アドレス

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての L2TP セッションのサマリーを表示する例を示します。

```
(Cisco Controller) > show l2tp summary
LAC_IPaddr LTid LSid RTid RSid ATid ASid State
---------- ---- ---- ---- ---- ---- ---- -----
```

show lag eth-port-hash

特定の MAC アドレスに使用する物理ポートを表示するには、**show lag eth-port-hash** コマンドを使用します。

show lag eth-port-hash *dest_MAC* ［*source_MAC*］

構文の説明

dest_MAC	非 IP パケットの出力ポートを決定する MAC アドレス。
source_MAC	（任意）非 IP パケットの出力ポートを決定する MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、特定の MAC アドレスに使用する物理ポートを表示する例を示します。

```
(Cisco Controller) > show lag eth-port-hash 11:11:11:11:11:11
Destination MAC 11:11:11:11:11:11 currently maps to port 1
```

show lag ip-port-hash

特定の IP アドレスに使用する物理ポートを表示するには、**show lag ip-port-hash** コマンドを使用します。

show lag ip-port-hash *dest_IP* [*source_IP*]

構文の説明

dest_IP	IP パケットの出力ポートを決定する IP アドレス。
source_IP	（任意）IP パケットの出力ポートを決定する IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは IPv4 および IPv6 の両方のアドレスをサポートします。

使用上のガイドライン

CAPWAP パケットの場合、アクセス ポイントの IP アドレスを入力します。EOIP パケットの場合、コントローラの IP アドレスを入力します。WIRED_GUEST パケットの場合、その IP アドレスを入力します。WLC からのトンネリングされていない IP パケットの場合、宛先 IP アドレスを入力します。その他のトンネリングされていない IP パケットの場合、宛先 IP アドレスと送信元 IP アドレスの両方を入力します。

このコマンドは、IPv4 と IPv6 の両方のアドレスに適用されます。

次に、特定の IP アドレスに使用する物理ポートを表示する例を示します。

```
(Cisco Controller) > show lag ip-port-hash 192.168.102.138
Destination IP 192.168.102.138 currently maps to port 1
```

show lag summary

現在のリンク集約（LAG）ステータスを表示するには、**show lag summary** コマンドを使用します。

show lag summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LAG 設定の現在のステータスを表示する例を示します。

```
(Cisco Controller) > show lag summary
LAG Enabled
```

show ldap

特定の Lightweight Directory Access Protocol（LDAP）サーバの LDAP サーバ情報を表示するには、**show ldap** コマンドを使用します。

show ldap *index*

構文の説明

index	LDAP サーバ インデックス。有効な値は、1 ～ 17 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LDAP サーバの詳細情報を表示する例を示します。

```
(Cisco Controller) > show ldap 1
Server Index..................................... 1
Address.......................................... 2.3.1.4
Port............................................. 389
Enabled.......................................... Yes
User DN.......................................... name1
User Attribute................................... attr1
User Type........................................ username1
Retransmit Timeout............................... 3 seconds
Bind Method ..................................... Anonymous
```

関連コマンド

config ldap

config ldap add

config ldap simple-bind

show ldap statistics

show ldap summary

show ldap statistics

すべての Lightweight Directory Access Protocol（LDAP）サーバ情報を表示するには、**show ldap statistics** コマンドを使用します。

show ldap statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LDAP サーバの統計情報を表示する例を示します。

```
(Cisco Controller) > show ldap statistics
Server Index..................................... 1
Server statistics:
  Initialized OK................................. 0
  Initialization failed.......................... 0
  Initialization retries......................... 0
  Closed OK...................................... 0
Request statistics:
  Received....................................... 0
  Sent........................................... 0
  OK............................................. 0
  Success........................................ 0
  Authentication failed.......................... 0
  Server not found............................... 0
  No received attributes......................... 0
  No passed username............................. 0
  Not connected to server........................ 0
  Internal error................................. 0
  Retries........................................ 0
Server Index..................................... 2
...
```

関連コマンド

config ldap

config ldap add

config ldap simple-bind

show ldap

show ldap summary

show ldap summary

現在の LDAP サーバのステータスを表示するには、**show ldap summary** コマンドを使用します。

show ldap summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、設定済みの LDAP サーバのサマリーを表示する例を示します。

```
(Cisco Controller) > show ldap summary
Idx   Server Address    Port   Enabled
---   ---------------  ----   -------
1     2.3.1.4          389    Yes
2     10.10.20.22      389    Yes
```

関連コマンド

config ldap

config ldap add

config ldap simple-bind

show ldap statistics

show ldap

show license all

Cisco WLC 上のすべてのライセンス情報を表示するには、**show license all** コマンドを使用します。

show license all

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、すべてのライセンスを表示する例を示します。

```
> show license all
License Store: Primary License Storage
StoreIndex:  0  Feature: wplus-ap-count   Version: 1.0
        License Type: Permanent
        License State: Inactive
        License Count: 12/0/0
        License Priority: Medium
StoreIndex:  1  Feature: base   Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
StoreIndex:  2  Feature: wplus   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
License Store: Evaluation License Storage
StoreIndex:  0  Feature: wplus   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  6 weeks  6 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  1  Feature: wplus-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  2 weeks  3 days
            Expiry date: Thu Jun 25 18:09:43 2009
        License Count: 250/250/0
        License Priority: High
StoreIndex:  2  Feature: base   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  3 days
```

```
        License Count: 250/0/0
        License Priority: Low
```

次に、スマート ライセンスのメカニズム上のすべてのライセンスを表示する例を示します。

```
(Cisco Controller) > show license all


Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: vWLC-Prod
  Virtual Account: Default
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Dec 11 12:19:38 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jun 08 12:19:37 2016 UTC
  Registration Expires: Dec 10 12:16:56 2016 UTC

License Authorization:
  Status: AUTHORIZED on Dec 11 12:20:12 2015 UTC
  Last Communication Attempt: SUCCEEDED on Dec 11 12:20:12 2015 UTC
  Next Communication Attempt: Jan 10 12:20:11 2016 UTC
  Communication Deadline: Mar 10 12:17:43 2016 UTC

--More-- or (q)uit

License Usage
==============

No licenses in use

Product Information
===================
UDI: PID:AIR-CTVM-K9,SN:91U8NQ5XDBE

Agent Version
=============
Smart Agent for Licensing: 1.4.0_rel/25
Component Versions: SA:1.4, SI:0.1, CH:rel_1, PK:x.x
```

show license capacity

Cisco 5500 シリーズ コントローラでこのライセンスに許可されるアクセス ポイントの最大数、コントローラに現在結合されているアクセス ポイント数、およびコントローラにさらに結合できるアクセス ポイント数を表示するには、**show license capacity** コマンドを使用します。

show license capacity

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、ライセンス機能を表示する例を示します。

```
> show license capacity
Licensed Feature    Max Count         Current Count     Remaining Count
-------------------------------------------------------------------------
AP Count            250               47                203
```

関連コマンド

license install

show license all

show license detail

show license feature

show license image-level

show license summary

license modify priority

show license evaluation

show license detail

Cisco 5500 シリーズ コントローラ上の特定ライセンスの詳細を表示するには、**show license detail** コマンドを使用します。

show license detail *license-name*

構文の説明

license-name	特定のライセンスの名前。

コマンド デフォルト

なし。

次に、ライセンスの詳細を表示する例を示します。

```
> show license detail wplus
Feature: wplus           Period left: Life time
Index:  1       Feature: wplus   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
        Store Index: 2
        Store Name: Primary License Storage
Index:  2       Feature: wplus   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  6 weeks  6 days
        License Count: Non-Counted
        License Priority: Low
        Store Index: 0
```

関連コマンド

license install

show license agent

show license all

show license feature

show license image-level

show license summary

license modify priority

show license expiring

Cisco 5500 シリーズ コントローラ上で期限切れになるライセンスの詳細を表示するには、**show license expiring** コマンドを使用します。

show license expiring

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、期限切れになるライセンスの詳細を表示する例を示します。

```
> show license expiring
StoreIndex:  0  Feature: wplus   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  6 weeks  6 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  1  Feature: wplus-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  2 weeks  3 days
            Expiry date: Thu Jun 25 18:09:43 2009
        License Count: 250/250/0
        License Priority: High
StoreIndex:  2  Feature: base   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  3 days
        License Count: 250/0/0
        License Priority: Low
```

関連コマンド

license install

show license all

show license detail

show license in-use

show license summary

license modify priority

show license evaluation

show license evaluation

Cisco 5500 シリーズ コントローラ上の評価ライセンスの詳細を表示するには、**show license evaluation** コマンドを使用します。

show license evaluation

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、評価ライセンスの詳細を表示する例を示します。

```
> show license evaluation
StoreIndex:  0  Feature: wplus   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  6 weeks  6 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  1  Feature: wplus-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  2 weeks  3 days
            Expiry date: Thu Jun 25 18:09:43 2009
        License Count: 250/250/0
        License Priority: High
StoreIndex:  2  Feature: base   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  3 days
        License Count: 250/0/0
        License Priority: Low
```

関連コマンド

license install

show license all

show license detail

show license expiring

show license in-use

show license summary

license modify priority

show license feature

Cisco 5500 シリーズ コントローラのライセンス対応機能の要約を表示するには、**show license feature** コマンドを使用します。

show license feature

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、ライセンス対応機能を表示する例を示します。

```
> show license feature
        Feature name Enforcement  Evaluation  Clear Allowed  Enabled
               wplus          yes         yes            yes      yes
      wplus-ap-count          yes         yes            yes      yes
                base           no         yes            yes       no
       base-ap-count          yes         yes            yes       no
```

関連コマンド

license install

show license all

show license detail

show license expiring

show license image-level

show license in-use

show license summary

show license modify priority

show license evaluation

show license file

Cisco 5500 シリーズ コントローラのライセンス対応機能の要約を表示するには、**show license file** コマンドを使用します。

show license file

構文の説明

このコマンドには引数またはキーワードはありません。

次に、ライセンス ファイルの詳細を表示する例を示します。

```
> show license file
License Store: Primary License Storage
  Store Index: 0
    License: 11 wplus-ap-count 1.0 LONG NORMAL STANDALONE EXCL 12_KEYS INFINIT
             E_KEYS NEVER NEVER NiL SLM_CODE CL_ND_LCK NiL *1AR5NS7M5AD8PPU400
              NiL NiL NiL 5_MINS <UDI><PID>AIR-CT5508-K9</PID><SN>RFD000P2D27<
             /SN></UDI> Pe0L7tv8KDUqo:zlPe423S5wasgM8G,tTs0i,7zLyA3VfxhnIe5aJa
             m63lR5l8JM3DPkr4O2DI43iLlKn7jomo3RFl1LjMRqLkKhiLJ2tOyuftQSq2bCAO6
             nR3wIb38xKi3t$<WLC>AQEBIQAB//++mCzRUbOhw28vz0czAY0iAm7ocDLUMb9ER0
             +BD3w2PhNEYwsBN/T3xXBqJqfC+oKRqwInXo3s+nsLU7rOtdOxoIxYZAo3LYmUJ+M
             FzsqlhKoJVlPyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQFzhr10GYolVzdzfJf
             EPQIx6tZ++/Vtc/q3SF/5Ko8XCY=</WLC>
    Comment:
       Hash: iOGjuLlXgLhcTB113ohIzxVioHA=
. . .
```

関連コマンド

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license in-use

show license summary

show license evaluation

show license handle

Cisco 5500 シリーズ コントローラ上のライセンス ハンドルを表示するには、**show license handle** コマンドを使用します。

show license handle

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次の例では、ライセンス ハンドルを表示する方法を示します。

```
> show license handle
Feature: wplus                            , Handle Count: 1
    Units: 01( 0), ID: 0x5e000001, NotifyPC: 0x1001e8f4 LS-Handle (0x00000001),
Units: ( 1)
    Registered clients: 1
        Context 0x1051b610, epID 0x10029378
Feature: base                             , Handle Count: 0
    Registered clients: 1
        Context 0x1053ace0, epID 0x10029378
Feature: wplus-ap-count                   , Handle Count: 1
    Units: 250( 0), ID: 0xd4000002, NotifyPC: 0x1001e8f4        LS-Handle (0x000
00002), Units: (250)
    Registered clients: None
Feature: base-ap-count                    , Handle Count: 0
    Registered clients: None
Global Registered clients: 2
               Context 0x10546270, epID 0x100294cc
               Context 0x1053bae8, epID 0x100294cc
```

関連コマンド

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license in-use

show license summary

show license image-level

Cisco 5500 シリーズ コントローラで使用されているライセンスのイメージ レベルを表示するには、**show license image-level** コマンドを使用します。

show license image-level

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、イメージ レベルのライセンス設定を表示する例を示します。

```
> show license image-level
Module name  Image level  Priority  Configured  Valid license
wnbu         wplus        1         YES         wplus
             base         2         NO
 NOTE: wplus includes two additional features: Office Extend AP, Mesh AP.
```

関連コマンド

license install

show license all

show license detail

show license expiring

show license feature

license modify priority

show license in-use

show license summary

show license in-use

Cisco 5500 シリーズ コントローラで使用されているライセンスを表示するには、**show license in-use** コマンドを使用します。

show license in-use

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、使用中のライセンスを表示する例を示します。

```
> show license in-use
StoreIndex:  2  Feature: wplus   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
StoreIndex:  1  Feature: wplus-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  2 weeks  3 days
            Expiry date: Thu Jun 25 18:09:43 2009
        License Count: 250/250/0
        License Priority: High
```

関連コマンド

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license modify priority

show license summary

show license permanent

show license evaluation

show license permanent

Cisco 5500 シリーズ コントローラ上の永久ライセンスを表示するには、**show license permanent** コマンドを使用します。

show license permanent

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、永久ライセンスの情報を表示する例を示します。

```
> show license permanent
StoreIndex:  0  Feature: wplus-ap-count   Version: 1.0
        License Type: Permanent
        License State: Inactive
        License Count: 12/0/0
        License Priority: Medium
StoreIndex:  1  Feature: base   Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
StoreIndex:  2  Feature: wplus   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
```

関連コマンド

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license in-use

show license summary

license modify priority

show license evaluation

show license status

シスコ ワイヤレス コントローラのライセンス ステータスを表示するには、**show license status** コマンドを使用します。

show license status

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、RTUライセンスのメカニズム上の**ライセンス ステータス**を表示する例を示します。

```
> show license status
               License Type Supported
        permanent  Non-expiring node locked license
        extension  Expiring node locked license
        evaluation Expiring non node locked license
               License Operation Supported
        install    Install license
        clear      Clear license
        annotate   Comment license
        save       Save license
        revoke     Revoke license
               Device status
        Device Credential type: DEVICE
        Device Credential Verification: PASS
        Rehost Type: DC_OR_IC
```

次に、スマートライセンスのメカニズム上の**ライセンス ステータス**を表示する例を示します。

```
(Cisco Controller) >show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: vWLC-Prod
  Virtual Account: Default
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Dec 11 12:19:38 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jun 08 12:19:37 2016 UTC
  Registration Expires: Dec 10 12:16:56 2016 UTC

License Authorization:
  Status: AUTHORIZED on Dec 11 12:20:12 2015 UTC
  Last Communication Attempt: SUCCEEDED on Dec 11 12:20:12 2015 UTC
  Next Communication Attempt: Jan 10 12:20:11 2016 UTC
  Communication Deadline: Mar 10 12:17:43 2016 UTC
```

show license statistics

Cisco 5500 シリーズ コントローラ上のライセンス統計情報を表示するには、**show license statistics** コマンドを使用します。

show license statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、ライセンス統計情報を表示する例を示します。

```
> show license statistics
                Administrative statistics
        Install success count:       0
        Install failure count:       0
        Install duplicate count:     0
        Comment add count:           0
        Comment delete count:        0
        Clear count:                 0
c        Save count:                  0
        Save cred count:             0
                Client status
        Request success count     2
        Request failure count     0
        Release count             0
        Global Notify count       0
```

関連コマンド

license install

show license all

show license detail

show license expiring

show license feature

show license image-level

show license in-use

show license summary

license modify priority

show license evaluation

show license summary

Cisco WLC 上のすべてのライセンスの簡単な要約を表示するには、**show license summary** コマンドを使用します。

show license summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、すべてのライセンスの簡単な要約を表示する例を示します。

```
> show license summary
Index 1 Feature: wplus
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: wplus-ap-count
        Period left:  2 weeks  3 days
        License Type: Evaluation
        License State: Active, In Use
        License Count: 250/250/0
        License Priority: High
Index 3 Feature: base
        Period left: Life time
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
Index 4 Feature: base-ap-count
        Period left:  8 weeks  3 days
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
        License Count: 250/0/0
        License Priority: Low
```

次に、スマートライセンスのメカニズム上の**ライセンス サマリー**を表示する例を示します。

```
(Cisco Controller) >show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: vWLC-Prod
  Virtual Account: Default
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Jun 08 12:19:38 2016 UTC

License Authorization:
```

```
Status: AUTHORIZED
Last Communication Attempt: SUCCEEDED
Next Communication Attempt: Jan 10 12:20:11 2016 UTC
```

show license udi

Cisco WLC 上のライセンスの Unique Device Identifier（UDI; 固有デバイス識別情報）値を表示するには、**show license udi** コマンドを使用します。

show license udi

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、RTU ライセンスのメカニズム上のライセンスの UDI 値を表示する例を示します。

```
(Cisco Controller) > show license udi
Device# PID                   SN                    UDI
-------------------------------------------------------------------------------------
*0      AIR-CT5508-K9         RFD000P2D27           AIR-CT5508-K9:RFD000P2D27
```

次に、スマートライセンスのメカニズム上のライセンスの UDI 値を表示する例を示します。

```
(Cisco Controller) > show license udi

UDI: PID:AIR-CTVM-K9,SN:91U8NQ5XDBE
```

show license usage

ハンドルごとの権限の詳細と使用状況、ならびにその権限タグを表示するには、**show license usage** コマンドを使用します。

show license usage

コマンド履歴

リリース	変更内容
8.2	このコマンドはリリース 8.2 で導入されました。

次に、権限の詳細を表示する例を示します。

```
(Cisco Controller) >show license usage
```

show load-balancing

ロードバランシング機能のステータスを表示するには、**show load-balancing** コマンドを使用します。

show load-balancing

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、ロードバランスのステータスを表示する例を示します。

```
> show load-balancing
Aggressive Load Balancing..................... Enabled
Aggressive Load Balancing Window.............. 0 clients
Aggressive Load Balancing Denial Count........... 3
Statistics
Total Denied Count............................. 10 clients
Total Denial Sent.............................. 20 messages
Exceeded Denial Max Limit Count................ 0 times
None 5G Candidate Count........................ 0 times
None 2.4G Candidate Count..................... 0 times
```

関連コマンド

config load-balancing

show local-auth config

ローカル認証の設定情報を表示するには、**show local-auth config** コマンドを使用します。

show local-auth config

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ローカル認証の設定情報を表示する例を示します。

```
(Cisco Controller) > show local-auth config
User credentials database search order:
Primary ..................................... Local DB
Configured EAP profiles:
Name ........................................ fast-test
Certificate issuer ..................... default
Enabled methods ........................ fast
Configured on WLANs ................... 2
EAP Method configuration:
EAP-TLS:
Certificate issuer ..................... default
Peer verification options:
 Check against CA certificates ..... Enabled
 Verify certificate CN identity .... Disabled
 Check certificate date validity ... Enabled
EAP-FAST:
TTL for the PAC ........................ 3 600
Initial client message ................ <none>
Local certificate required ............ No
Client certificate required ........... No
Vendor certificate required ........... No
Anonymous provision allowed ........... Yes
Authenticator ID ..................... 7b7fffffff0000000000000000000000
Authority Information ................. Test
EAP Profile..................................... tls-prof
Enabled methods for this profile .......... tls
Active on WLANs ........................... 1 3EAP Method configuration:
EAP-TLS:
Certificate issuer used ............... cisco
Peer verification options:
 Check against CA certificates ..... disabled
```

```
Verify certificate CN identity .... disabled
Check certificate date validity ... disabled
```

関連コマンド

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth statistics

show local-auth statistics

ローカル拡張認証プロトコル（EAP）の認証統計情報を表示するには、**show local-auth statistics** コマンドを使用します。

show local-auth statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ローカル認証の証明書統計情報を表示する例を示します。

```
(Cisco Controller) > show local-auth statistics
Local EAP authentication DB statistics:
Requests received ............................... 14
Responses returned .............................. 14
Requests dropped (no EAP AVP) ................... 0
Requests dropped (other reasons) ................ 0
Authentication timeouts ......................... 0
Authentication statistics:
  Method          Success         Fail
  ------------------------------------
  Unknown               0            0
  LEAP                  0            0
  EAP-FAST              2               0
  EAP-TLS               0            0
  PEAP                  0            0
Local EAP credential request statistics:
Requests sent to LDAP DB ........................ 0
Requests sent to File DB ........................ 2
Requests failed (unable to send) ................ 0
Authentication results received:
  Success ....................................... 2
  Fail .......................................... 0
Certificate operations:
Local device certificate load failures .......... 0
Total peer certificates checked ................. 0
Failures:
  CA issuer check ............................... 0
  CN name not equal to identity ................. 0
  Dates not valid or expired .................... 0
```

関連コマンド

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth config

show local-auth certificates

show local-auth certificates

ローカル認証の証明書情報を表示するには、**show local-auth certificates** コマンドを使用します。

show local-auth certificates

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、ローカルに保存された認証の証明書情報を表示する例を示します。

```
(Cisco Controller) > show local-auth certificates
```

関連コマンド

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth config

show local-auth statistics

show logging

syslog ファシリティ ロギング パラメータとバッファの内容を表示するには、**show logging** コマンドを使用します。

show logging

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、現在の設定とバッファの詳細な内容を表示する例を示します。

```
(Cisco Controller) >show logging

(Cisco Controller) > config logging syslog host 10.92.125.52
System logs will be sent to 10.92.125.52 from now on

(Cisco Controller) > config logging syslog host 2001:9:6:40::623
System logs will be sent to 2001:9:6:40::623 from now on

(Cisco Controller) > show logging
Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level..... errors
 - Number of system messages logged..... 1316
 - Number of system messages dropped..... 6892
- Logging of debug messages to buffer ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Cache of logging  ..... Disabled
- Cache of logging time(mins) ..... 10080
- Number of over cache time log dropped  ..... 0
Logging to console :
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8243
- Logging of debug messages to console ..... Enabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
Logging to syslog :
- Syslog facility..... local0
- Logging of system messages to console :
 - Logging filter level..... disabled
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 8208
- Logging of debug messages to console ..... Enabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Logging of system messages to syslog :
```

```
 - Logging filter level..................... errors
 - Number of system messages logged..... 1316
 - Number of system messages dropped..... 6892
- Logging of debug messages to syslog ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
- Number of remote syslog hosts..... 2
- syslog over tls..... Disabled
  - Host 0..... 10.92.125.52
  - Host 1..... 2001:9:6:40::623
  - Host 2.....
Logging of RFC 5424..... Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file..... Disabled
- Number of debug messages logged..... 0
- Number of debug messages dropped..... 0
Logging of traceback..... Enabled
```

show logging config-history

リブート時から実行されるすべての **config** コマンドを表示するには、**show logging config-history** コマンドを使用します。このコマンドは、これらのコマンドの実行時のタイムスタンプ、発生順序、コマンド実行元、および実行されたコマンドの履歴など、Cisco WLC のリブート後やすべての設定をクリアした後に失われる情報を理解するのに便利です。

show logging config-history

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
8.8	このコマンドが導入されました。

show logging flags

既存のフラグを表示するには、**show logging flags** コマンドを使用します。

show logging flags *AP* | *Cilent*

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、現在のフラグの詳細を表示する例を示します。

```
> show logging flags
ID    username     Connection From   Idle Time    Login Time
-- ---------------  ---------------  ------------  ------------
00 admin            EIA-232          00:00:00      00:19:04
```

関連コマンド

config logging flags close

show loginsession

既存のセッションを表示するには、**show loginsession** コマンドを使用します。

show loginsession

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、現在のセッションの詳細を表示する例を示します。

```
> show loginsession
ID    username     Connection From   Idle Time    Session Time
-- ---------------  ---------------  ------------  ------------
00 admin            EIA-232          00:00:00      00:19:04
```

関連コマンド

config loginsession close

show macfilter

MAC フィルタ パラメータを表示するには、**show macfilter** コマンドを使用します。

show macfilter {**summary** | **detail***MAC* | **mesh** | {**wlan** *wlan-id*}}

構文の説明

summary	すべての MAC フィルタ エントリの要約を表示します。
detail *MAC*	MAC フィルタ エントリの詳細を表示します。
mesh	すべての MESH AP MAC フィルタ エントリの要約を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

RADIUS サーバに送信される MAC アドレスの MAC デリミタ（なし、コロン、またはハイフン）が表示されます。MAC フィルタ テーブルには、無線 LAN とのアソシエートが常に許可されるクライアントが表示されます。

次に、MAC フィルタ エントリの詳細を表示する例を示します。

```
(Cisco Controller) >show macfilter detail xx:xx:xx:xx:xx:xx
MAC Address..................................... xx:xx:xx:xx:xx:xx
WLAN Identifier................................. Any
Interface Name.................................. management
Description..................................... RAP
```

次に、MAC フィルタ パラメータのサマリーを表示する例を示します。

```
(Cisco Controller) > show macfilter summary
MAC Filter RADIUS Compatibility mode.............. Cisco ACS
MAC Filter Delimiter.............................. None
Local Mac Filter Table
MAC Address               WLAN Id          Description
-----------------------   --------------   --------------------------------
xx:xx:xx:xx:xx:xx         Any              RAP
xx:xx:xx:xx:xx:xx         Any              PAP2 (2nd hop)
xx:xx:xx:xx:xx:xx         Any              PAP1 (1st hop)
```

show mdns ap summary

マルチキャスト ドメイン ネーム システム（mDNS）転送が有効になっているすべてのアクセス ポイントを表示するには、**show mnds ap summary** コマンドを使用します。

show mdns ap summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

次に、**show mnds ap summary** コマンドの出力例を示します。

```
(Cisco Controller) > show mdns ap summary

Number of mDNS APs............................. 2

AP Name              Ethernet MAC       Number of Vlans     VlanIdentifiers
---------           ----------------    -----------------   ------------------
ap-3500             cc:ef:48:72:0d:d9           0               Not applicable
ap-3600             00:22:bd:df:04:68           2                124,122
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *12 : show mdns ap summary* のフィールドの説明

フィールド	説明
AP Name	mDNS アクセス ポイント（mDNS 転送が有効になっているアクセス ポイント）の名前。
Ethernet MAC	mDNS アクセス ポイントの MAC アドレス。
Number of VLANs	アクセス ポイントが有線側から mDNS アドバタイズメントをスヌーピングする VLAN の数。アクセス ポイント 1 つで最大 10 個の VLAN をスヌーピングすることができます。
VLAN Identifiers	アクセスポイントがスヌーピングを行う VLAN の識別子。

show mdns domain-name-ip summary

マルチキャスト ドメイン ネーム システム（mDNS）ドメイン名の要約を表示するには、**show mdns domain-name-ip summary** コマンドを使用します。

show mdns domain-name-ip summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

使用上のガイドライン

各サービス アドバタイズメントには、サービス プロバイダーのドメイン名を IP アドレスにマッピングするレコードが含まれています。マッピングには、クライアントの MAC アドレス、VLAN ID、存続可能時間（TTL）、および IPv4 アドレスなどの詳細情報も含まれています。

次に、**show mdns domain-name-ip summary** コマンドの出力例を示します。

```
(Cisco Controller) > show mdns domain-name-ip summary

Number of Domain Name-IP Entries..... 1

DomainName      MAC Address          IP Address        Vlan Id Type   TTL   Time left

                                                     (in seconds) (in seconds)
-------------   -------------        -----------       -------------------- ------

tixp77.local.   00:50:b6:4f:69:70    209.165. 202.128   999    mDNSAP 4725   906
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *13 : show mdns domain-name-ip summary* のフィールドの説明

フィールド	説明
Domain Name	サービス プロバイダーのドメイン名。
MAC Address	サービス プロバイダーの MAC アドレス。
IP Address	サービス プロバイダーの IP アドレス。
VLAN ID	サービス プロバイダーの VLAN ID。

フィールド	説明
Type	次のいずれかのサービス提供元： • 有線 • ワイヤレス • 有線ゲスト • mDNS AP
TTL	サービスプロバイダーによって提供されるサービスの有効性を決定する TTL 値（秒）。TTL が期限切れになると、サービス プロバイダーは Cisco Wireless LAN Controller から削除されます。
Time Left	サービス プロバイダーが Cisco WLC から削除されるまでの残り時間（秒）。

show mdns profile

mDNS プロファイル情報を表示するには、**show mdns profile** コマンドを使用します。

show mdns profile {**summary** | **detailed** *profile-name*}

構文の説明

summary	mDNS プロファイルの要約を表示します。
detailed	mDNS プロファイルの詳細を表示します。
profile-name	mDNS プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。

次に、すべての mDNS プロファイルの要約を表示する例を示します。

```
> show mdns profile summary
Number of Profiles.............................. 2

ProfileName                       No. Of Services
--------------------------------  ---------------
default-mdns-profile                   5
profile1                               2
```

次に mDNS プロファイルの詳細を表示する例を示します。

```
> show mdns profile detailed default-mdns-profile

Profile Name.................................... default-mdns-profile
Profile Id...................................... 1
No of Services.................................. 5
Services........................................ AirPrint
                                                 AppleTV
                                                 HP_Photosmart_Printer_1
                                                 HP_Photosmart_Printer_2
                                                 Printer

No. Interfaces Attached......................... 0
No. Interface Groups Attached................... 0
No. Wlans Attached.............................. 1
Wlan Ids........................................ 1
```

関連コマンド

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

config mdns profile

show mdns ap

config mdns ap

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

show mdns service

マルチキャスト ドメイン ネーム システム（mDNS）サービス情報を表示するには、**show mnds service** コマンドを使用します。

show mdns service {**summary** | **detailed** *service-name* | **not-learnt**}

構文の説明

summary	すべての mDNS サービスの要約を表示します。
detailed	mDNS サービスの詳細を表示します。
service-name	mDNS サービスの名前。
not-learnt	コントローラで受信されたが、サービス クエリ ステータスが無効になっていたために検出されなかったすべてのサービス アドバタイズメントの要約を表示します。 学習されないすべての VLAN と発信元タイプのサービス アドバタイズメントが出力に表示されます。上位 500 のサービスがサマリー リストに表示されます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.4	このコマンドが導入されました。
7.5	**not-learnt** キーワードが追加されました。

次に、**show mnds summary** コマンドの出力例を示します。

```
Device > show mdns service summary

Number of Services.............................. 5

Service-Name              LSS  Origin     No SP Service-string
------------------------  ---------------  ------    --------
AirPrint                  Yes  Wireless    1      _ipp._tcp.local.
AppleTV                   Yes  Wireless    1      _airplay._tcp.local.
HP_Photosmart_Printer_1   Yes  Wireless    1      _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2   No   Wired       0      _cups._sub._ipp._tcp.local.
Printer                   No   Wired       0      _printer._tcp.local.
```

次に、**show mnds service detailed** コマンドの出力例を示します。

```
Device > show mdns service detailed AirPrint

Service Name.................................... AirPrint
Service Id...................................... 1
Service query status............................ Enabled
```

```
Service LSS status.............................. Disabled
Service learn origin............................ Wired
Number of Profiles.............................. 2
Profile......................................... student-profile, guest-profile


Number of Service Providers ..................... 2

Service Provider MAC-Address   AP Radio MAC    VLAN ID  Type     TTL   Time left
---------------- -----------   ------------    -------  ----     ----------------
user1         60:33:4b:2b:a6:9a -----              104  Wired    4500    4484
laptopa       00:21:1b:ea:36:60 3c:ce:73:1e:69:20  105  Wireless 4500    4484

Number of priority MAC addresses ................ 1

Sl.No        MAC Address         AP group name
-----    -------------------    --------------
1           44:03:a7:a3:04:45    AP_floor1
```

次に、**show mnds service not-learnt** コマンドの出力例を示します。

```
Device > show mdns service not-learnt

Number of Services.............................. 4

Origin      VLAN     TTL     TTL left   Client MAC            AP-MAC
Service-string
                               (sec)     (sec)
----------  ------  ------   ------   ------------------  ------------------
----------------------
Wireless     106      120     105      00:21:6a:76:88:04   04:da:d2:b3:11:00
100.106.11.9.in-addr.arpa.
Wireless     106      120     112      00:21:6a:78:ff:82   04:da:d2:b3:11:00
102.106.11.9.in-addr.arpa.
Wireless     106      120     75        00:21:6a:78:ff:82   04:da:d2:b3:11:00
108.104.11.9.in-addr.arpa.
Wireless     106      120     119      00:21:6a:78:ff:82   04:da:d2:b3:11:00
_airplayit._tcp.local.
```

show media-stream client

特定のメディア ストリーム クライアントまたは一連のクライアントの詳細を表示するには、**show media-stream client** コマンドを使用します。

show media-stream client {*media-stream_name* | **summary**}

構文の説明

media-stream_name	詳細が表示されるメディア ストリーム クライアントの名前。
summary	メディア ストリーム クライアント セットの詳細を表示します。

コマンド デフォルト

なし。

次に、メディア ストリーム クライアントの要約を表示する例を示します。

```
> show media-stream client summary
Number of Clients............................... 1
Client Mac         Stream Name  Stream Type  Radio WLAN  QoS    Status
-----------------  -----------  -----------  ----  ----  ------ -------
00:1a:73:dd:b1:12  mountainview  MC-direct    2.4   2     Video  Admitted
```

関連コマンド

show media-stream group summary

show media-stream group detail

特定のメディア ストリーム グループの詳細を表示するには、**show media-stream group detail** コマンドを使用します。

show media-stream group detail *media-stream_name*

構文の説明

media-stream_name	メディア ストリーム グループの名前。

コマンド デフォルト

なし。

次に、メディア ストリーム グループ設定の詳細を表示する例を示します。

```
> show media-stream group detail abc
Media Stream Name.............................. abc
Start IP Address............................... 227.8.8.8
End IP Address................................. 227.9.9.9
 RRC Parameters
 Avg Packet Size(Bytes)........................ 1200
 Expected Bandwidth(Kbps)...................... 300
 Policy........................................ Admit
 RRC re-evaluation............................. periodic
 QoS........................................... Video
 Status........................................ Multicast-direct
 Usage Priority................................ 5
 Violation..................................... drop
```

関連コマンド

show media-stream group summary

show media-stream group summary

メディア ストリームとクライアント情報のサマリーを表示するには、**show media-stream group summary** コマンドを使用します。

show media-stream group summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、メディア ストリーム グループのサマリーを表示する例を示します。

```
(Cisco Controller) > show media-stream group summary
Stream Name   Start IP       End IP         Operation Status
------------- -------------- -------------- ----------------
abc           227.8.8.8      227.9.9.9      Multicast-direct
```

関連コマンド

show 802.11 media-stream client

show media-stream client

show media-stream group detail

show mesh ap

メッシュ アクセス ポイントの設定を表示するには、**show mesh ap** コマンドを使用します。

show mesh ap {**summary** | **tree**}

構文の説明

summary	名前、モデル、ブリッジ仮想インターフェイス（BVI）のMACアドレス、米国コンピュータ緊急事態対策チーム（US-CERT）の MAC アドレス、ホップ、ブリッジ グループ名を含むメッシュ アクセス ポイント情報の要約を表示します。
tree	名前、ホップ カウンタ、リンクの信号対雑音比（SNR）、ブリッジ グループ名を含むメッシュ アクセス ポイント情報の要約をツリー構成で表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、要約形式を表示する例を示します。

```
(Cisco Controller) >show mesh ap summary
AP Name AP Model             BVI MAC              CERT MAC        Hop    Bridge Group
Name
------------------  -------------------  -----------------  ------------------   -----
 --
SB_RAP1 AIR-LAP1522AG-A-K9   00:1d:71:0e:d0:00  00:1d:71:0e:d0:00   0      sbox
SB_MAP1 AIR-LAP1522AG-A-K9   00:1d:71:0e:85:00  00:1d:71:0e:85:00   1      sbox
SB_MAP2 AIR-LAP1522AG-A-K9   00:1b:d4:a7:8b:00  00:1b:d4:a7:8b:00   2      sbox
SB_MAP3 AIR-LAP1522AG-A-K9   00:1d:71:0d:ee:00  00:1d:71:0d:ee:00   3      sbox
Number of Mesh APs.............................. 4
Number of RAPs.................................. 1
Number of MAPs.................................. 3
```

次に、階層（ツリー）形式で設定を表示する例を示します。

```
(Cisco Controller) >show mesh ap tree
 ========================================================
||  AP Name [Hop Counter, Link SNR, Bridge Group Name] ||
 ========================================================
[Sector 1]
----------
SB_RAP1[0,0,sbox]
  |-SB_MAP1[1,32,sbox]
    |-SB_MAP2[2,27,sbox]
      |-SB_MAP3[3,30,sbox]
--------------------------------------------------------
```

```
Number of Mesh APs.............................. 4
Number of RAPs.................................. 1
Number of MAPs.................................. 3
-----------------------------------------------------
```

show mesh astools stats

屋外メッシュ アクセス ポイントの孤立防止統計情報を表示するには、**show mesh astools stats** コマンドを使用します。

show mesh astools stats ［*cisco_ap* ］

構文の説明

cisco_ap	（任意）指定されたメッシュ アクセス ポイントの孤立防止機能統計情報。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての屋外メッシュ アクセス ポイントの孤立防止統計情報を表示する例を示します。

```
(Cisco Controller) >show mesh astools stats
Total No of Aps stranded : 0
```

次に、アクセス ポイント *sb_map1* の孤立防止統計情報を表示する例を示します。

```
(Cisco Controller) >show mesh astools stats sb_map1
Total No of Aps stranded : 0
```

show mesh backhaul

現在のバックホールを調べるには、**show mesh backhaul** コマンドを使用します。

show mesh backhaul *cisco_ap*

構文の説明

cisco_ap	アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、現在のバックホールを表示する例を示します。

```
(Cisco Controller) >show mesh backhaul
```

現在のバックホールが 5 GHz の場合、出力は次のとおりです。

```
Basic Basic Attributes for Slot  0
    Radio Type..................................... RADIO_TYPE_80211g
    Radio Role..................................... DOWNLINK ACCESS
    Administrative State .......................... ADMIN_ENABLED
    Operation State ............................... UP
      Current Tx Power Level ..................... 1
If the current backhaul is 2.4 GHz, the output is as follows:
Basic Attributes for Slot  1
    Radio Type..................................... RADIO_TYPE_80211a
    Radio Subband.................................. RADIO_SUBBAND_ALL
    Radio Role..................................... DOWNLINK ACCESS
    Administrative State .......................... ADMIN_ENABLED
    Operation State ............................... UP
      Current Tx Power Level ..................... 1
      Current Channel ............................ 165
      Antenna Type................................ EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBm units).... 0
Current Channel.................................6
Antenna Type....................................Externa_ANTENNA
External Antenna Gain (in .5 dBm units)...........0
```

show mesh cac

メッシュネットワークで使用されているまたは使用可能なコールアドミッション制御（CAC）トポロジおよび帯域幅を表示するには、**show mesh cac** コマンドを使用します。

show mesh cac {**summary** | {**bwused** {**voice** | **video**} | **access** | **callpath** | **rejected**} *cisco_ap* }

構文の説明

summary	各メッシュアクセスポイントに使用する音声コールと音声帯域幅の総数を表示します。
bwused	ツリートポロジで選択したアクセスポイントの帯域幅を表示します。
voice	使用されているまたは使用可能なメッシュ トポロジおよび音声帯域幅を表示します。
video	使用されているまたは使用可能なメッシュ トポロジおよびビデオ帯域幅を表示します。
access	ツリー トポロジで進行中のアクセス音声コールを表示します。
callpath	メッシュ ツリーに分散されたコール帯域幅を表示します。
rejected	ツリー トポロジで帯域幅不足のために拒否された音声コールを表示します。
cisco_ap	メッシュ アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コール アドミッション制御の設定の概要を表示する例を示します。

```
(Cisco Controller) >show mesh cac summary
AP Name              Slot#    Radio  BW Used/Max  Calls
-----------------  -------  -----  -----------  -----
SB_RAP1              0        11b/g   0/23437      0
                     1        11a     0/23437      0
SB_MAP1              0        11b/g   0/23437      0
                     1        11a     0/23437      0
SB_MAP2              0        11b/g   0/23437      0
                     1        11a     0/23437      0
SB_MAP3              0        11b/g   0/23437      0
                     1        11a     0/23437      0
```

次に、使用されているまたは使用可能なメッシュ トポロジおよび音声帯域幅を表示する例を示します。

```
(Cisco Controller) >show mesh cac bwused voice SB_MAP1
AP Name                Slot#    Radio      BW Used/Max
-------------         -------  -----      -----------
    SB_RAP1              0      11b/g       0/23437
                         1      11a         0/23437
|   SB_MAP1              0      11b/g       0/23437
                         1      11a         0/23437
||  SB_MAP2              0      11b/g       0/23437
                         1      11a         0/23437
||| SB_MAP3              0      11b/g       0/23437
                         1      11a         0/23437
```

次に、ツリー トポロジで進行中のアクセス音声コールを表示する例を示します。

```
(Cisco Controller) >show mesh cac access 1524_Map1
    AP Name             Slot#   Radio     Calls
    -------------      -------  -----     -----
    1524_Rap             0      11b/g      0
                         1      11a        0
                         2      11a        0
|   1524_Map1            0      11b/g      0
                         1      11a        0
                         2      11a        0
||  1524_Map2            0      11b/g      0
                         1      11a        0
                         2      11a        0
```

show mesh client-access

バックホール クライアント アクセス設定を表示するには、**show mesh client-access** コマンドを使用します。

show mesh client-access

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、メッシュ アクセス ポイントのバックホール クライアント アクセス設定を表示する例を示します。

```
(Cisco Controller) >show mesh client-access
Backhaul with client access status: enabled
Backhaul with client access extended status(3 radio AP): disabled
```

show mesh config

メッシュ設定を表示するには、**show mesh config** コマンドを使用します。

show mesh config

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	メッシュ コンバージェンス方式を含むようにディスプレイが拡張されました。

次に、グローバル メッシュ設定を表示する例を示します。

```
(Cisco Controller) >show mesh config
Mesh Range..................................... 12000
Mesh Statistics update period.................. 3 minutes
Backhaul with client access status............. disabled
Backhaul with extended client access status..... disabled
Background Scanning State...................... enabled
Backhaul Amsdu State........................... disabled
Mesh Security
   Security Mode............................... EAP
   External-Auth............................... disabled
   Use MAC Filter in External AAA server....... disabled
   Force External Authentication.............. disabled
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
   Association Interval........................ 60 minutes
   Parent Change Numbers....................... 3
Parent Change Interval..................... 60 minutes
Mesh Multicast Mode............................ In-Out
Mesh Full Sector DFS........................... enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... disabled
Mesh DCA channels for serial backhaul APs........ enabled
Mesh Slot Bias................................. enabled
Mesh Convergence Method........................ standard
```

show mesh convergence

メッシュ コンバージェンス設定を表示するには、**show mesh convergence** コマンドを使用します。

show mesh convergence

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。

次に、メッシュ コンバージェンス設定を表示する例を示します。

```
ap_console >show mesh convergence
Convergence method: fast
Subset channels: 157 165
Num.of Subset channels: 2

Mesh Convergence Global Data
old_conv_method: standard
 updated_subset: 1 subset_chan_seek: 1
```

show mesh env

メッシュ ネットワークのグローバルまたは特定の環境の要約情報を表示するには、**show mesh env** コマンドを使用します。

show mesh env {**summary** | *cisco_ap* }

構文の説明

summary	グローバル環境の要約情報を表示します。
cisco_ap	環境の要約情報が要求されるアクセス ポイントの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、グローバル環境の要約情報を表示する例を示します。

```
(Cisco Controller) >show mesh env summary
AP Name             Temperature(C)  Heater   Ethernet  Battery
------------------  --------------  ------   --------  -------
ap1130:5f:be:90      N/A             N/A      DOWN     N/A
AP1242:b2.31.ea      N/A             N/A      DOWN     N/A
AP1131:f2.8d.92      N/A             N/A      DOWN     N/A
AP1131:46f2.98ac     N/A             N/A      DOWN     N/A
ap1500:62:39:70      -36             OFF      UP       N/A
```

次に、アクセス ポイントの環境の要約を表示する例を示します。

```
(Cisco Controller) >show mesh env SB_RAP1
AP Name..................................... SB_RAP1
AP Model.................................... AIR-LAP1522AG-A-K9
AP Role..................................... RootAP
Temperature................................. 21 C, 69 F
Heater...................................... OFF
Backhaul.................................... GigabitEthernet0
GigabitEthernet0 Status..................... UP
    Duplex.................................. FULL
    Speed................................... 100
    Rx Unicast Packets...................... 114754
    Rx Non-Unicast Packets.................. 1464
    Tx Unicast Packets...................... 9630
    Tx Non-Unicast Packets.................. 3331
GigabitEthernet1 Status..................... DOWN
  POE Out................................... OFF
Battery..................................... N/A
```

show mesh neigh

メッシュアクセスポイントのメッシュネイバーに関する要約または詳細情報を表示するには、**show mesh neigh** コマンドを使用します。

show mesh neigh {**detail** | **summary**} {*cisco_ap* | **all**}

構文の説明

detail	指定したメッシュアクセスポイントとそのネイバー間のチャネルおよび信号対雑音比（SNR）の詳細を表示します。
summary	指定したメッシュ アクセス ポイントのメッシュ ネイバーを表示します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべてのアクセス ポイントを表示します。

（注） AP 自体が **all** キーワードで設定されている場合、**all** キーワードのアクセス ポイントは、**all** という名前の AP よりも優先されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントのネイバーのサマリーを表示する例を示します。

```
(Cisco Controller) >show mesh neigh summary RAP1
AP Name/Radio Mac Channel Rate  Link-Snr  Flags      State
----------------- ------- ----- -------- --------   --------
00:1D:71:0F:CA:00 157      54     6        0x0        BEACON
00:1E:14:48:25:00 157      24     1        0x0        BEACON
MAP1-BB00         157      54     41       0x11       CHILD BEACON
```

次に、アクセス ポイントの詳細なネイバー統計情報を表示する例を示します。

```
(Cisco Controller) >show mesh neigh detail RAP1
AP MAC : 00:1E:BD:1A:1A:00 AP Name: HOR1522_MINE06_MAP_S_Dyke
backhaul rate 54
FLAGS : 860 BEACON
worstDv 255, Ant 0, channel 153, biters 0, ppiters 0
Numroutes 0, snr 0, snrUp 8, snrDown 8, linkSnr 8
adjustedEase 0, unadjustedEase 0
txParent 0, rxParent 0
poorSnr 0
lastUpdate 2483353214 (Sun Aug 4 23:51:58 1912)
parentChange 0
Per antenna smoothed snr values: 0 0 0 0
Vector through 00:1E:BD:1A:1A:00
```

次の表に、**show mesh neigh detail** コマンドで表示される出力フラグを示します。

表 *14 : show mesh neigh detail* コマンドの出力フラグ

出力フラグ	説明
AP MAC	指定したメッシュ アクセス ポイントのメッシュ ネイバーの MAC アドレス。
AP Name	メッシュ アクセス ポイントの名前。
FLAGS	隣接を表示します。表示される値は次のとおりです。 • UPDATED：最近更新されたネイバー。 • NEIGH：上位ネイバーの 1 つ。 • EXCLUDED：ネイバーは現在除外されています。 • WASEXCLUDED：ネイバーは除外リストから最近削除されました。 • PERMSNR：永続的な SNR のネイバー。 • CHILD：子のネイバー。 • PARENT：親のネイバー。 • NEEDUPDATE：最新のネイバーではないため更新が必要です。 • BEACON：このネイバーからビーコンが聞こえました。 • ETHER：イーサネットのネイバー。
worstDv	ネイバーから最も離れたディスタンス ベクトル。
Ant	ルートが受信されたアンテナ。
channel	ネイバーのチャネル。
biters	ブラック リストのタイムアウト残余数。
ppiters	潜在的な親のタイムアウト残余数。
Numroutes	ディスタンス ルートの数。
snr	信号対雑音比

出力フラグ	説明
snrUp	AP へのリンクの SNR。
snrDown	AP からのリンクの SNR。
linkSnr	リンクの計算された SNR。
adjustedEase	この AP を経由したルート AP への容易度。現在の SNR およびしきい値および SNR 値に基づきます。
unadjustedEase	ホップ数を適切に適用した後の、この AP を経由したルート AP への容易度。
txParent	このノードが親の間に送信されるパケット。
rxparent	このノードが親の間に受信したパケット。
poorSnr	ノードから不良 SNR を受信するパケット。
lastUpdate	このネイバーについて最後に受信されたメッセージのタイムスタンプ
parentChange	このノードが最後に親になったとき。
per antenna smoother SNR values	SNR 値はアンテナ 0 だけに入力されます。

show mesh path

メッシュアクセスポイントとそのネイバー間のリンクのチャネルおよび信号対雑音比（SNR）の詳細を表示するには、**show mesh path** コマンドを使用します。

show mesh path *cisco_ap*

構文の説明

cisco_ap	メッシュ アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、指定したリンク パスのチャネルおよび SNR の詳細を表示する例を示します。

```
(Cisco Controller) >show mesh path mesh-45-rap1
AP Name/Radio Mac Channel Rate  Link-Snr  Flags      State
----------------- ------- ----- -------- --------   --------
MAP1-BB00         157      54     32       0x0       UPDATED NEIGH PARENT BEACON
RAP1              157      54     37       0x0        BEACON
```

show mesh per-stats

特定のメッシュアクセスポイントのネイバーから送信されたパケットのパケットエラーのパーセンテージを表示するには、**show mesh per-stats** コマンドを使用します。

show mesh per-stats summary {*cisco_ap* | **all**}

構文の説明

summary	パケット エラー率の統計を表示します。
cisco_ap	メッシュ アクセス ポイントの名前。
all	すべてのメッシュ アクセス ポイントが表示されます。

（注） AP 自体が **all** キーワードで設定されている場合、**all** キーワードのアクセス ポイントは、**all** という名前の AP よりも優先されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

パケットエラーのパーセンテージは1（正常に送信されたパケット数を送信された合計パケット数で割った値）です。

次に、メッシュ アクセス ポイントのネイバーから送信されたパケットのパケット エラーのパーセンテージを表示する例を示します。

```
(Cisco Controller) >show mesh per-stats summary ap_12
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted:               104833
Total Packets transmitted successfully: 104833
Total Packets retried for transmission: 33028
RTS Attempts:                            0
RTS Success:                             0
Neighbor MAC Address:                    00:0B:85:80:ED:D0
Total Packets transmitted:               0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
Neighbor MAC Address:                    00:17:94:FE:C3:5F
Total Packets transmitted:               0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
RTS Attempts:                            0
RTS Success:                             0
```

show mesh public-safety

4.8 GHz Public Safety 設定を表示するには、**show mesh public-safety** コマンドを使用します。

show mesh public-safety

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、4.8 GHz Public Safety 設定を表示する例を示します。

```
(Cisco Controller) >(Cisco Controller) >show mesh public-safety
Global Public Safety status: disabled
```

show mesh queue-stats

メッシュ アクセス ポイントのクライアント アクセス キューのパケット数をタイプ別に表示するには、**show mesh queue-stats** コマンドを使用します。

show mesh queue-stats {*cisco_ap* | **all**}

（注） AP 自体が **all** キーワードで設定されている場合、**all** キーワードのアクセス ポイントは、**all** という名前の AP よりも優先されます。

構文の説明

cisco_ap	パケット キュー統計情報を表示したいアクセス ポイントの名前。
all	すべてのアクセス ポイントを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイント ap417 のパケット キュー統計情報を表示する例を示します。

```
(Cisco Controller) >show mesh queue-stats ap417
Queue Type Overflows Peak length Average length
---------- --------- ----------- --------------
Silver     0         1           0.000
Gold       0         4           0.004
Platinum   0         4           0.001
Bronze     0         0           0.000
Management 0         0           0.000
```

show mesh security-stats

特定のアクセス ポイントのパケット エラー統計情報を表示するには、**show mesh security-stats** コマンドを使用します。

show mesh security-stats {*cisco_ap* | **all**}

構文の説明

cisco_ap	パケット エラー統計情報を表示したいアクセス ポイントの名前。
all	すべてのアクセス ポイントを表示します。

（注） AP 自体が **all** キーワードで設定されている場合、**all** キーワードのアクセス ポイントは、**all** という名前の AP よりも優先されます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、特定アクセス ポイントとその子のパケット エラー統計情報と、アソシエーション、認証、再アソシエーション、再認証についての失敗、タイムアウト、および成功のカウントを表示します。

次に、アクセス ポイント ap417 のパケット エラー統計情報を表示する例を示します。

```
(Cisco Controller) >show mesh security-stats ap417
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
x Packets 14, Rx Packets 19, Rx Error Packets 0
Parent-Side Statistics:
-------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Child-Side Statistics:
-------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
```

```
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

show mesh stats

アクセス ポイントのメッシュ統計情報を表示するには、**show mesh stats** コマンドを使用します。

show mesh stats *cisco_ap*

構文の説明

cisco_ap	アクセス ポイント名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクセス ポイントの統計情報を表示する例を示します。

```
(Cisco Controller) >show mesh stats RAP_AP1
RAP in state Maint
rxNeighReq 759978, rxNeighRsp 568673
txNeighReq 115433, txNeighRsp 759978
rxNeighUpd 8266447 txNeighUpd 693062
tnextchan 0, nextant 0, downAnt 0, downChan 0, curAnts 0
tnextNeigh 0, malformedNeighPackets 244, poorNeighSnr 27901
blacklistPackets 0, insufficientMemory 0
authenticationFailures 0
Parent Changes 1, Neighbor Timeouts 16625
```

show mgmtuser

Cisco Wireless LAN Controller のローカル管理ユーザ アカウントを表示するには、**show mgmtuser** コマンドを使用します。

show mgmtuser

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、管理ユーザのリストを表示する例を示します。

```
> show mgmtuser
User Name                Permissions    Description           Password Strength
-----------------------  ------------   --------------        ------------------
admin                    read-write                                 Weak
```

関連コマンド

config mgmtuser add

config mgmtuser delete

config mgmtuser description

config mgmtuser password

show mobility anchor

Cisco Wireless LAN Controller モビリティ グループの無線 LAN アンカー エクスポート リストを表示するには、または特定の WLAN または有線ゲスト LAN のモビリティ アンカーとして設定されたコントローラのリストとステータスを表示するには、**show mobility anchor** コマンドを使用します。

show mobility anchor ［**wlan** *wlan_id* ｜ **guest-lan** *guest_lan_id*］

構文の説明

wlan	（任意）無線 LAN モビリティ グループの設定を表示します。
wlan_id	1 ～ 512 の無線 LAN 識別子（両端の値を含む）。
guest-lan	（任意）ゲスト LAN モビリティ グループの設定を表示します。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子（両端の値を含む）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

[status] フィールドの出力（例を参照）には、次のいずれかの値が表示されます。

- UP：コントローラはアクセス可能で、データを渡すことができます。
- CNTRL_PATH_DOWN：mpings に失敗しました。コントロール パス経由でコントローラにアクセスできないため、エラーが発生したと見なされます。
- DATA_PATH_DOWN：epings に失敗しました。コントローラにアクセスできないため、エラーが発生したと見なされます。
- CNTRL_DATA_PATH_DOWN：mpings および epings の両方に失敗しました。コントローラにアクセスできないため、エラーが発生したと見なされます。

次に、モビリティ無線 LAN アンカー リストを表示する例を示します。

```
(Cisco Controller) >show mobility anchor
Mobility Anchor Export List
 WLAN ID     IP Address            Status
 -------     ---------------       ------
 12           192.168.0.15         UP
```

```
GLAN ID     IP Address            Status
-------     ---------------       -------
1           192.168.0.9           CNTRL_DATA_PATH_DOWN
```

show mobility ap-list

モビリティ AP リストを表示するには、**show mobility ap-list** コマンドを使用します。

show mobility ap-list

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ AP リストを表示する例を示します。

（注） AP名は新しいモビリティでのみ表示されます。古いモビリティでは、AP名はUnknownと表示されます。

```
(Cisco Controller) >show mobility ap-list
AP Name                      AP Radio MAC address      Controller          Learnt From
---------------------------  ----------------------   ---------------   ----------------
AP30e4.dbc5.38ab              b8:62:1f:e5:33:10         9.7.104.10           Self
```

show mobility foreign-map

モビリティ無線 LAN の外部マップ リストを表示するには、**show mobility foreign-map** コマンドを使用します。

show mobility foreign-map wlan *wlan_id*

構文の説明

wlan	モビリティ WLAN の外部マップ リストを表示します。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、モビリティ無線 LAN に外部マップ リストを取得する例を示します。

```
(Cisco Controller) >show mobility foreign-map wlan 2
Mobility Foreign Map List
 WLAN ID               Foreign MAC Address                Interface
 -------               -------------------                ---------
   2                    00:1b:d4:6b:87:20                 dynamic-105
```

show mobility group member

同じドメイン内のモビリティ グループ メンバの詳細を表示するには、**show mobility group member** コマンドを使用します。

show mobility group member hash

構文の説明

hash	同じドメイン内のモビリティ グループ メンバのハッシュ キーを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、モビリティ グループ メンバのハッシュ キーを表示する例を示します。

```
(Cisco Controller) >show mobility group member hash
Default Mobility Domain..................... new-mob

 IP Address      Hash Key
-------------------------------------------------------------

 9.2.115.68      a819d479dcfeb3e0974421b6e8335582263d9169

 9.6.99.10       0974421b6e8335582263d9169a819d479dcfeb3e

 9.7.7.7         feb3e0974421b6e8335582263d9169a819d479dc
```

show mobility oracle

Mobility Oracle（MO）に既知のモビリティ コントローラのステータスを表示する、またはMO クライアント データベースの詳細を表示するには、**show mobility oracle** コマンドを使用します。

show mobility oracle {**client** {**detail** | **summary**} | **summary**}

構文の説明

client	MO クライアント データベースを表示します。
detail	MO クライアントデータベース内のクライアントに関する詳細を表示します。
summary	MO データベースの要約を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.3.112.0	このコマンドが導入されました。

次に、**show mobility oracle summary** コマンドの出力例を示します。

```
(Cisco Controller) >show mobility oracle summary

Number of MCs..................................... 2

IP Address       MAC Address        Link Status        Client Count
---------------  -----------------  -----------------  -------------

9.71.104.10       88:43:e1:7d:fe:00  Control Path Down  0
9.71.104.250      e8:b7:48:a2:16:e0  Up                 2
```

次に、**show mobility oracle client summary** コマンドの出力例を示します。

```
(Cisco Controller) >show mobility oracle client summary

Number of Clients................................ 2

MAC Address       Anchor MC             Foreign MC        AssocTime
----------------- --------------------- ----------------- --------------

00:18:de:b0:5c:91 9.72.104.250           -                   0
00:1e:e5:f9:c9:e2 9.72.104.250           -                   0
```

次に、**show mobility oracle client detail** コマンドの出力例を示します。

```
(Cisco Controller) >show mobility oracle client detail 00:1e:e5:f9:c9:e2

Client MAC Address : ............................ 00:1e:e5:f9:c9:e2
Client IP address : ............................. 0.0.0.0
Anchor MC IP address : .......................... 9.71.104.250
```

```
Anchor MC NAT IP address : ..................... 9.71.104.250
Foreign MC IP address : ........................ -
Foreign MC NAT IP address : .................... -
Client Association Time : ...................... 0
Client Entry update timestamp : ................ 1278543135.0
```

show mobility statistics

Cisco Wireless LAN Controller モビリティ グループの統計情報を表示するには、**show mobility statistics** コマンドを使用します。

show mobility statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Mobility Manager の統計情報を表示する例を示します。

```
(Cisco Controller) >show mobility statistics
Global Mobility Statistics
   Rx Errors..................................... 0
   Tx Errors..................................... 0
   Responses Retransmitted....................... 0
   Handoff Requests Received..................... 0
   Handoff End Requests Received................. 0
   State Transitions Disallowed.................. 0
   Resource Unavailable.......................... 0
Mobility Initiator Statistics
   Handoff Requests Sent......................... 0
   Handoff Replies Received...................... 0
   Handoff as Local Received..................... 2
   Handoff as Foreign Received................... 0
   Handoff Denys Received........................ 0
   Anchor Request Sent........................... 0
   Anchor Deny Received.......................... 0
   Anchor Grant Received......................... 0
   Anchor Transfer Received...................... 0
Mobility Responder Statistics
   Handoff Requests Ignored...................... 0
   Ping Pong Handoff Requests Dropped............ 0
   Handoff Requests Dropped...................... 0
   Handoff Requests Denied....................... 0
   Client Handoff as Local....................... 0
   Client Handoff as Foreign  ................... 0
   Client Handoff Inter Group ................... 0
   Anchor Requests Received...................... 0
   Anchor Requests Denied........................ 0
   Anchor Requests Granted....................... 0
   Anchor Transferred............................ 0
```

show mobility summary

Cisco WLC モビリティ グループの要約情報を表示するには、**show mobility summary** コマンドを使用します。

show mobility summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

WLAN コントローラの中には、モビリティ セキュリティ モードが表示されないものがあります。

次に、**show mobility summary** コマンドの出力例を示します。

```
(Cisco Controller) >show mobility summary

Symmetric Mobility Tunneling (current) ..... Disabled
Symmetric Mobility Tunneling (after reboot) ..... Disabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... snmp_gui
Multicast Mode ..... Disabled
Mobility Domain ID for 802.11r..... 0x66bd
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 1
Mobility Control Message DSCP Value..... 0
Controllers configured in the Mobility Group
MAC Address        IP Address       Group Name         Multicast IP  Status
00:1b:d4:6b:87:20    1.100.163.70     snmp_gui         0.0.0.0        Up
```

次に、新しいモビリティ アーキテクチャでの **show mobility summary** コマンドの出力例を示します。

```
(Cisco Controller) >show mobility summary

Mobility Protocol Port..... 16666
Default Mobility Domain..... Mobility
Multicast Mode ..... Disabled
Mobility Domain ID for 802.11r..... 0xb348
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 3
Mobility Control Message DSCP Value..... 0

Controllers configured in the Mobility Group
 IP Address  Public IP Address  Group Name     Multicast IP  MAC Address
```

```
Status
 9.71.106.2  9.72.106.2         Mobility      0.0.0.0      00:00:00:00:00:00  Control
and Data Path Down
 9.71.106.3  9.72.106.3         Mobility      0.0.0.0      00:00:00:00:00:00  Control
and Data Path Down
 9.71.106.69 9.72.106.69        Mobility      0.0.0.0      68:ef:bd:8e:5f:20
Up
```

show msglog

Cisco WLC データベースに書き込まれたメッセージ ログを表示するには、**show msglog** コマンドを使用します。

show msglog

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

使用上のガイドライン

15 エントリを超える場合は、例に示すメッセージを表示するよう求められます。

次に、メッセージ ログを表示する例を示します。

```
(Cisco Controller) >show msglog
Message Log Severity Level..................... ERROR
Thu Aug  4 14:30:08 2005  [ERROR] spam_lrad.c 1540: AP 00:0b:85:18:b6:50 associated.
Last AP failure was due to Link Failure
Thu Aug  4 14:30:08 2005  [ERROR] spam_lrad.c 13840: Updating IP info for AP 00:
0b:85:18:b6:50 -- static 0, 1.100.49.240/255.255.255.0, gtw 1.100.49.1
Thu Aug  4 14:29:32 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Thu Aug  4 14:29:32 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a switch group
 reset
Thu Aug  4 14:29:32 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Thu Aug  4 14:29:22 2005  [ERROR] sim.c 2841: Unable to get link state for primary port
 0 of interface ap-manager
Thu Aug  4 14:29:22 2005  [ERROR] dtl_l2_dot1q.c 767: Unable to get USP
Thu Aug  4 14:29:22 2005  Previous message occurred 2 times
Thu Aug  4 14:29:14 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake called with
 NULL pointer: osapi_bsntime.c:927
Thu Aug  4 14:29:14 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake called with
 NULL pointer: osapi_bsntime.c:919
Thu Aug  4 14:29:14 2005  [CRITICAL] hwutils.c 1861: Security Module not found
Thu Aug  4 14:29:13 2005  [CRITICAL] bootos.c 791: Starting code...
```

show nac statistics

Cisco Wireless LAN Controller の詳細なネットワーク アクセス コントロール（NAC）情報を表示するには、**show nac statistics** コマンドを使用します。

show nac statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ネットワーク アクセス コントロール設定の詳細な統計情報を表示する例を示します。

```
(Cisco Controller) > show nac statistics
Server Index..................................................... 1
Server Address.....................................................
xxx.xxx.xxx.xxx
Number of requests sent.......................................... 0
Number of retransmissions........................................ 0
Number of requests received...................................... 0
Number of malformed requests received............................ 0
Number of bad auth requests received............................. 0
Number of pending requests....................................... 0
Number of timed out requests..................................... 0
Number of misc dropped request received.......................... 0
Number of requests sent.......................................... 0
```

関連コマンド

show nac summary

config guest-lan nac

config wlan nac

debug nac

show nac summary

Cisco Wireless LAN Controller の NAC 要約情報を表示するには、**show nac summary** コマンドを使用します。

show nac summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ネットワーク アクセス コントロール設定の要約情報を表示する例を示します。

```
(Cisco Controller) > show nac summary
NAC ACL Name ..............................................
Index  Server Address                            Port     State
-----  ----------------------------------------  ----     -----
1      xxx.xxx.xxx.xxx                           13336    Enabled
```

関連コマンド

show nac statistics

config guest-lan nac

config wlan nac

debug nac

show network

すべての WLAN の 802.3 ブリッジの現在のステータスを表示するには、**show network** コマンドを使用します。

show network

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、ネットワークの詳細を表示する例を示します。

```
(Cisco Controller) > show network
```

関連コマンド

config network

show network summary

show network multicast mgid detail

show network multicast mgid summary

show network summary

Cisco Wireless LAN Controller のネットワーク構成を表示するには、**show network summary** コマンドを使用します。

show network summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、要約設定を表示する例を示します。

```
(Cisco Controller) >show network summary
RF-Network Name............................. RF
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Web Mode RC4 Cipher Preference....... Disable
OCSP........................................ Disabled
OCSP responder URL..........................
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
Ethernet Multicast Forwarding............... Disable
Ethernet Broadcast Forwarding............... Disable
AP Multicast/Broadcast Mode................. Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
IGMP Query Interval......................... 20 seconds
MLD snooping................................ Disabled
MLD timeout................................. 60 seconds
MLD query interval.......................... 20 seconds
User Idle Timeout........................... 300 seconds
AP Join Priority............................ Disable
ARP Idle Timeout............................ 300 seconds
ARP Unicast Mode............................ Disabled
Cisco AP Default Master..................... Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
Mesh Full Sector DFS........................ Enable
AP Fallback ................................ Disable
Web Auth CMCC Support ...................... Disabled
Web Auth Redirect Ports .................... 80
Web Auth Proxy Redirect  ................... Disable
Web Auth Captive-Bypass   .................. Disable
Web Auth Secure Web  ....................... Enable
Fast SSID Change ........................... Disabled
AP Discovery - NAT IP Only ................. Enabled
IP/MAC Addr Binding Check .................. Enabled
CCX-lite status ............................ Disable
oeap-600 dual-rlan-ports ................... Disable
```

```
oeap-600 local-network ..................... Enable
mDNS snooping.............................. Disabled
mDNS Query Interval........................ 15 minutes
Web Color Theme............................ Red
Web Color Theme............................ Default
CAPWAP Prefer Mode......................... IPv4
```

show netuser

ローカル ユーザ データベース内の特定のユーザの設定を表示するには、**show netuser** コマンドを使用します。

show netuser {**detail** *user_name* | **guest-roles** | **summary**}

構文の説明

detail	特定のネットワーク ユーザの詳細情報を表示します。
user_name	ネットワーク ユーザ。
guest_roles	ゲストユーザの設定済みロールを表示します。
summary	ローカル ユーザ データベース内のすべてのユーザの要約を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show netuser summary** コマンドの出力例を示します。

```
(Cisco Controller) > show netuser summary
Maximum logins allowed for a given username ........Unlimited
```

次に、**show netuser detail** コマンドの出力例を示します。

```
(Cisco Controller) > show netuser detail john10
username..................................... abc
WLAN Id...................................... Any
Lifetime..................................... Permanent
Description.................................. test user
```

関連コマンド

config netuser add

config netuser delete

config netuser description

config netuser guest-role apply

config netuser wlan-id

config netuser guest-roles

show netuser guest-roles

現在の Quality of Service（QoS）ロールとそれらの帯域幅パラメータのリストを表示するには、**show netuser guest-roles** コマンドを使用します。

show netuser guest-roles

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ゲストのネットワーク ユーザの QoS ロールを表示する例を示します。

```
(Cisco Controller) > show netuser guest-roles
Role Name............................. Contractor
 Average Data Rate.................... 10
 Burst Data Rate...................... 10
 Average Realtime Rate................ 100
 Burst Realtime Rate.................. 100
Role Name............................. Vendor
 Average Data Rate.................... unconfigured
 Burst Data Rate...................... unconfigured
 Average Realtime Rate................ unconfigured
 Burst Realtime Rate.................. unconfigured
```

関連コマンド

config netuser add

config netuser delete

config netuser description

config netuser guest-role apply

config netuser wlan-id

show netuser guest-roles

show netuser

show network multicast mgid detail

特定のマルチキャスト グループ ID（MGID）のマルチキャスト グループに結合されたすべてのクライアントを表示するには、**show network multicast mgid detail** コマンドを使用します。

show network multicast mgid detail *mgid_value*

構文の説明

mgid_value	550 ～ 4095 の範囲内の数。

コマンド デフォルト

なし。

次に、マルチキャスト データベースの詳細を表示する例を示します。

```
> show network multicast mgid detail
Mgid ............................... 550
Multicast Group Address ............ 239.255.255.250
Vlan ............................... 0
Rx Packet Count .................... 807399588
No of clients ...................... 1
Client List .......................
  Client MAC       Expire TIme (mm:ss)
   00:13:02:23:82:ad   0:20
```

関連コマンド

show network summary

show network multicast mgid detail

show network

show network multicast mgid summary

すべてのマルチキャスト グループと対応するマルチキャスト グループ ID（MGID）を表示するには、**show network multicast mgid summary** コマンドを使用します。

show network multicast mgid summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、マルチキャスト グループとそれらの MGID の要約を表示する例を示します。

```
> show network multicast mgid summary
Layer2 MGID Mapping:
--------------------
InterfaceName             vlanId     MGID
------------------------------ ------  -----
management              0      0
test             0    9
wired           20     8
Layer3 MGID Mapping:
--------------------
Number of Layer3 MGIDs ................. 1
 Group address           Vlan    MGID
 ------------------  -----   ------
 239.255.255.250         0      550
```

関連コマンド

show network summary

show network multicast mgid detail

show network

show network summary

ネットワーク コンフィギュレーション設定を表示するには、**show network summary** コマンドを使用します。

show network summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、ネットワーク サマリーで IPv6 マルチキャストの詳細を表示するように更新されました。

次に、**show ipv6 summary** コマンドの出力例を示します。

```
(Cisco Controller) >show network summary
RF-Network Name............................. johnny
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Web Mode RC4 Cipher Preference....... Disable
OCSP........................................ Disabled
OCSP responder URL..........................
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Forwarding............... Enable
Ethernet Broadcast Forwarding............... Enable
IPv4 AP Multicast/Broadcast Mode............ Multicast   Address : 239.9.9.9
IPv6 AP Multicast/Broadcast Mode............ Multicast   Address : ff1e::6:9
IGMP snooping............................... Enabled
IGMP timeout................................ 60 seconds
IGMP Query Interval......................... 20 seconds
MLD snooping................................ Enabled
MLD timeout................................. 60 seconds
MLD query interval.......................... 20 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Enable
Mgmt Via Dynamic Interface.................. Enable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Mesh Full Sector DFS........................ Enable
AP Fallback ................................ Enable
Web Auth CMCC Support ...................... Disabled
Web Auth Redirect Ports .................... 80
Web Auth Proxy Redirect  ................... Disable
Web Auth Captive-Bypass   .................. Disable
Web Auth Secure Web  ....................... Enable
```

```
Fast SSID Change ........................... Disabled
AP Discovery - NAT IP Only ................. Enabled
IP/MAC Addr Binding Check .................. Enabled
Link Local Bridging Status ................. Disabled
CCX-lite status ............................ Disable
oeap-600 dual-rlan-ports ................... Disable
oeap-600 local-network ..................... Enable
oeap-600 Split Tunneling (Printers)......... Disable
WebPortal Online Client .................... 0
WebPortal NTF_LOGOUT Client ................ 0
mDNS snooping............................... Disabled
mDNS Query Interval......................... 15 minutes
Web Color Theme............................. Default
L3 Prefer Mode.............................. IPv4
```

show nmsp notify-interval summary

Network Mobility Services Protocol（NMSP）構成の設定を表示するには、**show nmsp notify-interval summary** コマンドを使用します。

show nmsp notify-interval summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、NMSP 設定情報を表示する例を示します。

```
> show nmsp notify-interval summary
NMSP Notification Interval Summary
 Client
        Measurement interval:    2 sec
 RFID
        Measurement interval:    8 sec
 Rogue AP
        Measurement interval:    2 sec
 Rogue Client
        Measurement interval:    2 sec
```

関連コマンド

clear locp statistics

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp statistics

show nmsp status

show nmsp status

アクティブな NMSP 接続ステータスを表示するには、**show nmsp status** コマンドを使用します。

show nmsp status

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.3	このコマンドが導入されました。

次に、アクティブな nmsp 接続ステータスの例を示します。

```
(Cisco Controller) >show nmsp status
```

show nmsp statistics

ネットワークモビリティサービスプロトコル（NMSP）カウンタを表示するには、**show nmsp statistics** コマンドを使用します。

show nmsp statistics {**summary** | **connection all**}

構文の説明

summary	一般的な NMSP カウンタを表示します。
connection all	すべての接続別カウンタを表示します。

コマンド デフォルト

なし。

次に、一般的な NMSP カウンタの要約を表示する例を示します。

```
> show nmsp statistics summary
Send RSSI with no entry:                0
Send too big msg:                       0
Failed SSL write:                       0
Partial SSL write:                      0
SSL write attempts to want write:
Transmit Q full:0
Max Measure Notify Msg:                 0
Max Info Notify Msg:                    0
Max Tx Q Size:                          2
Max Rx Size:                            1
Max Info Notify Q Size:                 0
Max Client Info Notify Delay:           0
Max Rogue AP Info Notify Delay:         0
Max Rogue Client Info Notify Delay:     0
Max Client Measure Notify Delay:        0
Max Tag Measure Notify Delay:           0
Max Rogue AP Measure Notify Delay:      0
Max Rogue Client Measure Notify Delay: 0
Max Client Stats Notify Delay:          0
Max Tag Stats Notify Delay:             0
RFID Measurement Periodic :             0
RFID Measurement Immediate :            0
Reconnect Before Conn Timeout:          0
```

次に、すべての接続別 NMSP カウンタを表示する例を示します。

```
> show nmsp statistics connection all
NMSP Connection Counters
Connection 1 :
 Connection status:  UP
 Freed Connection:    0
 Nmsp Subscr Req:     0          NMSP Subscr Resp:   0
 Info Req:            1          Info Resp:          1
 Measure Req:         2          Measure Resp:        2
 Stats Req:           2          Stats Resp:          2
 Info Notify:         0          Measure Notify:      0
 Loc Capability:      2
 Location Req:        0          Location Rsp:        0
```

```
Loc Subscr Req:      0          Loc Subscr Rsp:      0
Loc Notif:           0
Loc Unsubscr Req:    0          Loc Unsubscr Rsp:    0
IDS Get Req:         0          IDS Get Resp:        0
IDS Notif:           0
IDS Set Req:         0          IDS Set Resp:        0
```

関連コマンド

show nmsp notify-interval summary

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp status

show nmsp subscription

コントローラ上でアクティブになっているネットワーク モビリティ サービス プロトコル（NMSP）サービスを表示するには、**show nmsp subscription** コマンドを使用します。

show nmsp subscription {**summary** | **detail** *ip-addr*}

構文の説明

summary	コントローラがサブスクライブされているすべての NMSP サービスを表示します。
detail	コントローラがサブスクライブされているすべての NMSP サービスの詳細を表示します。
ip-addr	特定の IPv4 または IPv6 アドレスでサブスクライブされている NMSP サービスについてのみ詳細を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、コントローラがサブスクライブされているすべての NMSP サービスの要約を表示する例を示します。

```
> show nmsp subscription summary
Mobility Services Subscribed:
Server IP          Services
---------          --------
10.10.10.31        RSSI, Info, Statistics
```

次に、すべての NMSP サービスの詳細を表示する例を示します。

```
> show nmsp subscription detail 10.10.10.31
Mobility Services Subscribed by 10.10.10.31
Services          Sub-services
--------          ------------
RSSI              Mobile Station, Tags,
Info              Mobile Station,
Statistics        Mobile Station, Tags,

> show nmsp subscription detail 2001:9:6:40::623
Mobility Services Subscribed by 2001:9:6:40::623
Services          Sub-services
--------          ------------
RSSI              Mobile Station, Tags,
```

```
Info              Mobile Station,
Statistics        Mobile Station, Tags,
```

show nmsp subscription summary

Mobility Services Engine によってコントローラに登録されたモビリティ サービスを表示するには、**show nmsp subscription summary** コマンドを使用します。

show nmsp subscription summary

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.3	このコマンドが導入されました。

次に、コントローラに登録されたモビリティ サービスの例を示します。

```
(Cisco Controller) >show nmsp subscription summary
```

show ntp-keys

ネットワーク タイム プロトコル認証キーの詳細を表示するには、**show ntp-keys** コマンドを使用します。

show ntp-keys

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、NTP 認証キーの詳細を表示する例を示します。

```
(Cisco Controller) > show ntp-keys
Ntp Authentication Key Details...................
      Key Index
     -----------
         1
         3
```

関連コマンド

config time ntp

show ntp-keys

ネットワーク タイム プロトコル認証キーの詳細を表示するには、**show ntp-keys** コマンドを使用します。

show ntp-keys

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、NTP 認証キーの詳細を表示する例を示します。

```
(Cisco Controller) > show ntp-keys
Ntp Authentication Key Details...................
      Key Index
     -----------
         1
         3
```

関連コマンド

config time ntp

show pmk-cache

ペアワイズ マスター キー（PMK）キャッシュの情報を表示するには、**show pmk-cache** コマンドを使用します。

show pmk-cache {**all** | *MAC*}

構文の説明

all	PMK キャッシュのすべてのエントリに関する情報を表示します。
MAC	PMK キャッシュの単一エントリに関する情報。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、PMK キャッシュの単一のエントリに関する情報を表示する例を示します。

```
(Cisco Controller) >show pmk-cache xx:xx:xx:xx:xx:xx
```

次に、PMK キャッシュのすべてのエントリに関する情報を表示する例を示します。

```
(Cisco Controller) >show pmk-cache all
PMK Cache
                   Entry
Station            Lifetime   VLAN Override          IP Override
-----------------  --------   --------------------   ---------------
```

show pmipv6 domain

PMIPv6 ドメインのサマリー情報を表示するには、 **show pmipv6 domain** コマンドを使用します。

show pmipv6 domain *domain_name* **profile** *profile_name*

構文の説明

domain_name	PMIPv6 ドメインの名前。ドメイン名は最大 127 文字の英数字で、大文字と小文字を区別します。
profile	PMIPv6 プロファイルを指定します。
profile_name	PMIPv6 ドメインに関連付けられたプロファイル名。プロファイル名は最大 127 文字の英数字で、大文字と小文字を区別します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、PMIPv6 ドメインのサマリー情報を表示する例を示します。

```
(Cisco Controller) >show pmipv6 domain floor1 profile profile1
NAI: @example.com
APN: Example
LMA: Examplelma

NAI: *
APN: ciscoapn
LMA: ciscolma
```

show pmipv6 mag bindings

Mobile Access Gateway（MAG）のバインディング情報を表示するには、 **show pmipv6 mag binding** コマンドを使用します。

show pmipv6 mag bindings［**lma** *lma_name* | **nai** *nai_string*］

構文の説明

lma	（任意）Local Mobility Anchor（LMA）に対する MAG のバインディングの詳細を表示します。
lma_name	LMA の名前。LMA 名は最大 127 文字の英数字で、大文字と小文字を区別します。
nai	（任意）クライアントに対する MAG のバインディングの詳細を表示します。
nai_string	クライアントのネットワーク アクセス ID（NAI）。NAI は最大 127 文字の英数字で、大文字と小文字を区別します。コロンを除くすべての特殊文字を使用できます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAG バインディングを表示する例を示します。

```
(Cisco Controller) >show pmipv6 mag binding
[Binding][MN]: Domain: D1, Nai: MN1@cisco.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: Management
        [Binding][MN]: Hoa: 0xE0E0E02, att: 3, llid: aabb.cc00.c800
        [Binding][MN][LMA]: Id: LMA1
        [Binding][MN][LMA]: lifetime: 3600
        [Binding][MN][GREKEY]: Upstream: 102, Downstream: 1
```

show pmipv6 mag globals

Mobile Access Gateway（MAG）の PMIPv6 グローバル パラメータを表示するには、**show pmipv6 mag globals** コマンドを使用します。

show pmipv6 mag globals

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MAG の PMIPv6 グローバル パラメータを表示する例を示します。

```
(Cisco Controller) >show pmipv6 mag globals
Domain  : D1

MAG Identifier  : M1
        MAG Interface                   : Management
        Max Bindings                    : 10000
        Registration Lifetime           : 3600 (sec)
        BRI Init-delay time             : 1000 (msec)
        BRI Max-delay time              : 2000 (msec)
        BRI Max retries                 : 1
        Refresh time                    : 300 (sec)
        Refresh RetxInit time           : 1000 (msec)
        Refresh RetxMax time            : 32000 (msec)
        Timestamp option                : Enabled
        Validity Window                 : 7
        Peer#1:
                LMA Name: AN-LMA-5K      LMA IP: 209.165.201.10
        Peer#2:
                LMA Name: AN-LMA         LMA IP: 209.165.201.4
        Peer#3:
                LMA Name: AN-LMA         LMA IP: 209.165.201.4
```

show pmipv6 mag stats

Mobile Access Gateway（MAG）の統計情報を表示するには、**show pmipv6 mag stats** コマンドを使用します。

show pmipv6 mag stats［**domain** *domain_name* **peer** *lma_name*］

構文の説明

domain	（任意）ドメインの Local Mobility Anchor（LMA）の MAG 統計情報を表示します。
domain_name	PMIPv6 ドメインの名前。ドメイン名は最大 127 文字の英数字で、大文字と小文字を区別します。
peer	（任意）LMA の MAG 統計情報を表示します。
lma_name	LMA の名前。LMA 名は最大 127 文字の英数字で、大文字と小文字を区別します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

次の表に、LMA 統計情報の説明を示します。

表 *15 : LMA* 統計情報の説明*:*

LMA 統計情報	説明
PBU Sent	MAG が LMA に送信する Proxy Binding Updates（PBU）の総数。 PBU は、MAG によってモバイル ノードの LMA に送信される要求メッセージです。このメッセージにより、モバイル ノードのインターフェイスと現在の気付アドレス（Proxy-CoA）間でバインディングが確立されます。
PBA Received	LMA から MAG が受信する Proxy Binding Acknowledgements（PBA）の総数。 PBA は、MAG から受信した PBU メッセージに対して、LMA から送信される応答メッセージです。
PBRI Sent	MAG が LMA に送信する Proxy Binding Revocation Indications（PBRI）の総数。
PBRI Received	MAG が LMA から受信する PBRI の総数。
PBRA Sent	MAG が LMA に送信する Proxy Binding Revocation Acknowledgements（PBRA）の総数。

LMA 統計情報	説明
PBRA Received	MAG が LMA から受信する PBRA の総数。
Number of Handoff	MAG と LMA 間のハンドオフの数。

次に、LMA 統計情報の表示方法の例を示します。

```
(Cisco Controller) >show pmipv6 mag stats
[M1]: Total Bindings    : 1
[M1]: PBU Sent          : 7
[M1]: PBA Rcvd          : 4
[M1]: PBRI Sent         : 0
[M1]: PBRI Rcvd         : 0
[M1]: PBRA Sent         : 0
[M1]: PBRA Rcvd         : 0
[M1]: No Of handoff     : 0
```

show pmipv6 profile summary

PMIPv6 プロファイルのサマリーを表示するには、 **show pmipv6 profile summary** コマンドを使用します。

show pmipv6 profile summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、PMIPv6 プロファイルのサマリーを表示する例を示します。

```
(Cisco Controller) >show pmipv6 profile summary
 Profile Name    WLAN IDS (Mapped)
 ------------    -----------------
  Group1            6
```

show policy

設定されているポリシーの要約と、ポリシーの詳細および統計情報を表示するには、**show policy** コマンドを使用します。

show policy {**summary** | *policy-name* [**statistics**]}

構文の説明

summary	設定されているポリシーの要約を表示します。
policy-name	ポリシーの名前。
statistics	（任意）ポリシーの統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

次に、**show policy summary** コマンドの出力例を示します。

```
(Cisco Controller) > show policy summary

Number of Policies..... 2

Policy Index Policy Name
------------ ----------------
1            student-FullAccess
2            teacher-FullAccess
```

次に、ポリシーの詳細を表示する例を示します。

```
(Cisco Controller) > show policy student-FullAccess

Policy Index..................................... 1
Match Role....................................... <none>
Match Eap Type................................... EAP-TLS
ACL.............................................. <none>
QOS.............................................. <none>
Average Data Rate................................ 0
Average Real Time Rate........................... 0
Burst Data Rate.................................. 0
Burst Real Time Rate............................. 0
Vlan Id.......................................... 155
Session Timeout.................................. 1800
Sleeping client timeout.......................... 12

Active Hours
------------
```

```
Start Time   End Time      Day
----------   --------      ---

Match Device Types
------------------
Android
```

次に、ポリシーの統計情報を表示する例を示します。

```
(Cisco Controller) > show policy student-FullAccess statistics

Policy Index..................................... student-FullAccess
Matching Attributes None......................... 619
No Policy Match.................................. 224
Device Type Match................................ 0
EAP Type Match................................... 0
Role Type Match.................................. 0
Client Disconnected.............................. 4
Acl Applied...................................... 0
Vlan changed..................................... 614
Session Timeout Applied.......................... 4
QoS Applied...................................... 0
Avg Data Rate Applied............................ 0
Avg Real Time Rate Applied....................... 0
Burst Data Rate Applied.......................... 0
Burst Real Time Rate Applied..................... 0
Sleeping-Client-Timeout Applied.................. 0
```

show port

Cisco Wireless LAN Controller のポート設定を個別にまたはグローバルに表示するには、**show port** コマンドを使用します。

show port {*port-number* | **summary** | **detailed-info** | **vlan**}

構文の説明

port-number	物理インターフェイスのポート番号。
summary	すべてのポートのサマリーを表示します。
detailed-info	詳細なポート情報を表示します。
vlan	VLAN ポート テーブルのサマリーを表示します。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、個別のワイヤレス LAN コントローラ ポートに関する情報を表示する例を示します。

```
(Cisco Controller) > show port 1
            STP   Admin   Physical   Physical   Link   Link    Mcast
Pr  Type   Stat   Mode    Mode     Status   Status  Trap   Appliance   POE
-- -------- ---- ------- ---------- ---------- ------ ------- ---------
 -------
1  Normal  Disa Enable  Auto       1000
Full  Down   Enable  Enable     N/A
```

（注） 一部の WLAN コントローラでは、マルチキャスト機能または Power over Ethernet（PoE）機能がサポートされていないため、これらの機能は表示されません。

次に、すべてのポートの要約を表示する例を示します。

```
(Cisco Controller) > show port summary
            STP   Admin   Physical   Physical   Link   Link    Mcast
Pr  Type   Stat   Mode    Mode     Status   Status  Trap   Appliance   POE
 SFPType
-- ------- ---- ------- ---------- ---------- ------ ------- ---------
 -------------
1  Normal  Forw Enable  Auto       1000
```

```
Full  Up     Enable  Enable     N/A NotPresent
2  Normal  Disa Enable  Auto       1000
Full  Down   Enable  Enable     N/A NotPresent
3  Normal  Disa Enable  Auto       1000
Full  Down   Enable  Enable     N/A NotPresent
4  Normal  Disa Enable  Auto       1000
Full  Down   Enable  Enable     N/A NotPresent
```

（注） 一部の WLAN コントローラは、ポートが 1 つしか表示されないことがありますが、それはポートが 1 つしかないためです。

show profiling policy summary

Cisco Wireless LAN Controller（WLC）のローカルデバイスの分類を表示するには、**show profiling policy summary** コマンドを使用します。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

次に、**show profiling policy summary** コマンドの出力例を示します。

```
(Cisco Controller) > show profiling policy summary

Number of Builtin Classification Profiles: 88
ID   Name                                               Parent Min CM
Valid
==== ================================================== ====== ======
=====
   0 Android                                              None     30
Yes
   1 Apple-Device                                         None     10
Yes
   2 Apple-MacBook                                           1     20
Yes
   3 Apple-iPad                                              1     20
Yes
   4 Apple-iPhone                                            1     20
Yes
   5 Apple-iPod                                              1     20
Yes
   6 Aruba-Device                                         None     10
Yes
   7 Avaya-Device                                         None     10
Yes
   8 Avaya-IP-Phone                                          7     20
Yes
   9 BlackBerry                                           None     20
Yes
  10 Brother-Device                                       None     10
Yes
  11 Canon-Device                                         None     10
Yes
  12 Cisco-Device                                         None     10
Yes
```

```
  13 Cisco-IP-Phone                                12      20
Yes
  14 Cisco-IP-Phone-7945G                          13      70
Yes
  15 Cisco-IP-Phone-7975                           13      70
Yes
  16 Cisco-IP-Phone-9971                           13      70
Yes
  17 Cisco-DMP                                     12      20
Yes
  18 Cisco-DMP-4400                                17      70
Yes
  19 Cisco-DMP-4310                                17      70
Yes
  20 Cisco-DMP-4305                                17      70
Yes
  21 DLink-Device                                  None    10
Yes
  22 Enterasys-Device                              None    10
Yes
  23 HP-Device                                     None    10
Yes
  24 HP-JetDirect-Printer                          23      30
Yes
  25 Lexmark-Device                                None    10
Yes
  26 Lexmark-Printer-E260dn                        25      30
Yes
  27 Microsoft-Device                              None    10
Yes
  28 Netgear-Device                                None    10
Yes
  29 NintendoWII                                   None    10
Yes
  30 Nortel-Device                                 None    10
Yes
  31 Nortel-IP-Phone-2000-Series                   30      20
Yes
  32 SonyPS3                                       None    10
Yes
  33 XBOX360                                       27      20
Yes
  34 Xerox-Device                                  None    10
Yes
  35 Xerox-Printer-Phaser3250                      34      30
Yes
  36 Aruba-AP                                       6      20
Yes
  37 Cisco-Access-Point                            12      10
Yes
  38 Cisco-IP-Conference-Station-7935              13      70
```

```
Yes
  39 Cisco-IP-Conference-Station-7936                  13     70
Yes
  40 Cisco-IP-Conference-Station-7937                  13     70
Yes
```

show qos

Quality of Service（QoS）情報を表示するには、**show qos** コマンドを使用します。

show qos {**bronze** | **gold** | **platinum** | **silver**}

構文の説明

bronze	WLAN の Bronze プロファイルの QoS 情報を表示します。
gold	WLANのゴールドプロファイルのQoS情報を表示します。
platinum	WLANのプラチナプロファイルのQoS情報を表示します。
silver	WLANのシルバープロファイルのQoS情報を表示します。

コマンド デフォルト

なし。

次に、ゴールド プロファイルの QoS 情報を表示する例を示します。

```
> show qos gold
Description..................................... For Video Applications
Maximum Priority................................ video
Unicast Default Priority........................ video
Multicast Default Priority...................... video
Per-SSID Rate Limits............................ UpstreamDownstream
Average Data Rate............................... 0 0
Average Realtime Data Rate...................... 0 0
Burst Data Rate................................. 0 0
Burst Realtime Data Rate........................ 0 0
Per-Client Rate Limits.......................... UpstreamDownstream
Average Data Rate............................... 0 0
Average Realtime Data Rate...................... 0 0
Burst Data Rate................................. 0 0
Burst Realtime Data Rate........................ 0 0
protocol........................................ none

802.11a Customized EDCA Settings:
ecwmin.......................................... 3
ecwmax.......................................... 4
aifs............................................ 7
txop............................................ 94

802.11a Customized packet parameter Settings:
Packet retry time............................... 3
Not retrying threshold.......................... 100
Disassociating threshold........................ 500
Time out value.................................. 35
```

関連コマンド

config qos protocol-type

show qos qosmap

現在の QoS マップ設定を表示するには、**show qos** コマンドを使用します。

show qos qosmap

構文の説明		
	qosmap	現在の QoS マップを表示します。

コマンド デフォルト	
	なし

コマンド履歴		
	リリース	変更内容
	8.1	このコマンドが導入されました。

次に、現在の QoS マップ設定の例を示します。

```
show qos qosmap
```

show queue-info

システムに関連するすべてのメッセージ キュー情報を表示するには、**show queue-info** コマンドを使用します。

show queue-info

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドが導入されました。

次に、**show queue-info** コマンドの出力例を示します。

```
(Cisco Controller) > show queue-info

Total message queue count = 123

Queue Name                    Allocated    InUse       MaxUsed
--------------------------------------------------------------
PRINTF-Q                        256          0          0
dtlqueue                        4096         0          6
GRE Queue                       100          0          1
dtlarpqueue                     4096         0          6
NIM-Q                           116          0          1
SIM-Q                           116          0          6
DHCP Client Queue               8            0          0
dhcpv6ProxyMsgQueue             250          0          0
FDQ-Q                           30300        0          3
dot1d_Queue                     512          0          29
Garp-Q                          256          0          1
dot3ad_queue                    1024         0          0
DEBUG-Q                         8192         0          8
LOGGER-Q                        8192         0          5
TS-Q                            256          0          0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *16 : show queue-info* フィールドの説明

フィールド	説明
Queue Name	タスクのメッセージ キューの名前。
Allocated	メッセージキューのメモリ サイズ（バイト単位）。

フィールド	説明
InUse	現在使用されているキュー。値 0 は、タスクによって処理される必要のあるメッセージが存在しないことを示します。
MaxUsed	コントローラの起動後にタスクによって処理されるメッセージの最大数。

show コマンド：r ～ z

- show radius acct detailed （1734 ページ）
- show radius acct statistics （1735 ページ）
- show radius auth detailed （1736 ページ）
- show radius auth statistics （1737 ページ）
- show radius avp-list （1738 ページ）
- show radius summary （1739 ページ）
- show redundancy interfaces （1740 ページ）
- show redundancy latency （1741 ページ）
- show redundancy mobilitymac （1742 ページ）
- show redundancy peer-route summary （1743 ページ）
- show redundancy peer-system statistics （1744 ページ）
- show redundancy statistics （1745 ページ）
- show redundancy summary （1746 ページ）
- show redundancy timers （1747 ページ）
- show remote-lan （1748 ページ）
- show reset （1750 ページ）
- show rfid client （1751 ページ）
- show rfid config （1752 ページ）
- show rfid detail （1753 ページ）
- show rfid summary （1754 ページ）
- show rf-profile summary （1755 ページ）
- show rf-profile details （1756 ページ）
- show rogue adhoc custom summary （1757 ページ）
- show rogue adhoc detailed （1758 ページ）
- show rogue adhoc friendly summary （1760 ページ）
- show rogue adhoc malicious summary （1761 ページ）
- show rogue adhoc unclassified summary （1762 ページ）
- show rogue adhoc summary （1763 ページ）
- show rogue ap clients （1764 ページ）

- show rogue ap custom summary （1766 ページ）
- show rogue ap detailed （1768 ページ）
- show rogue ap friendly summary （1771 ページ）
- show rogue ap malicious summary （1773 ページ）
- show rogue ap summary （1775 ページ）
- show rogue ap unclassified summary （1778 ページ）
- show rogue auto-contain （1779 ページ）
- show rogue client detailed （1780 ページ）
- show rogue client summary （1781 ページ）
- show rogue ignore-list （1782 ページ）
- show rogue rule detailed （1784 ページ）
- show rogue rule summary （1786 ページ）
- show route kernel （1787 ページ）
- show route summary （1788 ページ）
- show rules （1789 ページ）
- show run-config （1790 ページ）
- show run-config startup-commands （1791 ページ）
- show serial （1792 ページ）
- show sessions （1793 ページ）
- show snmpcommunity （1794 ページ）
- show snmpengineID （1795 ページ）
- show snmptrap （1796 ページ）
- show snmpv3user （1797 ページ）
- show snmpversion （1798 ページ）
- show spanningtree port （1799 ページ）
- show spanningtree switch （1800 ページ）
- show stats port （1801 ページ）
- show stats switch （1803 ページ）
- show switchconfig （1805 ページ）
- show sysinfo （1806 ページ）
- show system iostat （1807 ページ）
- show system top （1808 ページ）
- show tacacs acct statistics （1812 ページ）
- show tacacs athr statistics （1813 ページ）
- show tacacs auth statistics （1814 ページ）
- show tacacs summary （1815 ページ）
- show tech-support （1816 ページ）
- show time （1817 ページ）
- show trapflags （1819 ページ）
- show traplog （1821 ページ）
- show tunnel profile-summary （1822 ページ）

- show tunnel profile-detail （1823 ページ）
- show tunnel eogre-summary （1824 ページ）
- show tunnel eogre-statistics （1825 ページ）
- show tunnel eogre-domain-summary （1826 ページ）
- show tunnel eogre gateway （1827 ページ）
- show watchlist （1828 ページ）
- show wlan （1829 ページ）
- show wps ap-authentication summary （1834 ページ）
- show wps cids-sensor （1835 ページ）
- show wps mfp （1836 ページ）
- show wps shun-list （1837 ページ）
- show wps signature detail （1838 ページ）
- show wps signature events （1839 ページ）
- show wps signature summary （1841 ページ）
- show wps summary （1843 ページ）
- show wps wips statistics （1845 ページ）
- show wps wips summary （1846 ページ）
- show wps ap-authentication summary （1847 ページ）

show radius acct detailed

RADIUS アカウンティング サーバ情報を表示するには、**show radius acct detailed** コマンドを使用します。

show radius acct detailed *radius_index*

構文の説明

radius_index	RADIUS サーバ インデックス。範囲は 1 ～ 17 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、RADIUS アカウンティング サーバ情報を表示する例を示します。

```
(Cisco Controller) > show radius acct detailed 5

Radius Index.........5
NAI Realms..........LAB.VTV.BLR.cisco.co.in
```

show radius acct statistics

Cisco Wireless LAN Controller の RADIUS アカウンティング サーバの統計情報を表示するには、**show radius acct statistics** コマンドを使用します。

show radius acct statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS アカウンティング サーバの統計情報を表示する例を示します。

```
(Cisco Controller) > show radius acct statistics
Accounting Servers:
Server Index..................................... 1
Server Address................................... 10.1.17.10
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 0
Retry Requests................................... 0
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

関連コマンド

config radius acct

config radius acct ipsec authentication

config radius acct ipsec disable

config radius acct network

show radius auth statistics

show radius summary

show radius auth detailed

RADIUS 認証サーバ情報を表示するには、**show radius auth detailed** コマンドを使用します。

show radius auth detailed *radius_index*

構文の説明

radius_index	RADIUS サーバ インデックス。範囲は 1 ～ 17 です。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、RADIUS 認証サーバ情報を表示する例を示します。

```
(Cisco Controller) > show radius auth detailed 1

Radius Index........1
NAI Realms..........LAB.VTV.BLR.cisco.co.in
```

show radius auth statistics

Cisco Wireless LAN Controller の RADIUS 認証サーバの統計情報を表示するには、**show radius auth statistics** コマンドを使用します。

show radius auth statistics

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバの統計情報を表示する例を示します。

```
(Cisco Controller) > show radius auth statistics
Authentication Servers:
  Server Index..................................... 1
  Server Address................................... 209.165.200.10
  Msg Round Trip Time.............................. 0 (1/100 second)
  First Requests................................... 0
  Retry Requests................................... 0
  Accept Responses................................. 0
  Reject Responses................................. 0
  Challenge Responses.............................. 0
  Malformed Msgs................................... 0
  Bad Authenticator Msgs........................... 0
  Pending Requests................................. 0
  Timeout Requests................................. 0
  Unknowntype Msgs................................. 0
  Other Drops...................................... 0
```

関連コマンド

config radius auth

config radius auth management

config radius auth network

show radius summary

show radius avp-list

RADIUS VSA AVP を表示するには、**show radius avp-list** コマンドを使用します。

show radius avp-list *profile-name*

構文の説明		
	profile-name	ダウンロードした AVP を表示するプロファイル名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、RADIUS VSA AVP を表示する例を示します。

```
(Cisco Controller) > show radius avp-list
```

show radius summary

RADIUS 認証およびアカウンティング サーバのサマリーを表示するには、**show radius summary** コマンドを使用します。

show radius summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RADIUS 認証サーバのサマリーを表示する例を示します。

```
(Cisco Controller) > show radius summary
Vendor Id Backward Compatibility..................... Disabled
Credentials Caching.................................. Disabled
Call Station Id Type................................. IP Address
Administrative Authentication via RADIUS......... Enabled
Authentication Servers
Index  Type  Server Address    Port    State     Tout  RFC-3576  IPsec
 - AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----  ----  ---------------  ------  --------  ----  --------  --------------
---------------------------------
Accounting Servers
Index  Type  Server Address    Port    State     Tout  RFC-3576  IPsec
 - AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----  ----  ---------------  ------  --------  ----  --------  --------------
---------------------------------
```

関連コマンド

show radius auth statistics

show radius acct statistics

show redundancy interfaces

冗長性の詳細とサービス ポートの IP アドレスを表示するには、 **show redundancy interfaces** コマンドを使用します。

show redundancy interfaces

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、冗長性とサービス ポートの IP アドレス情報を表示する例を示します。

```
(Cisco Controller) >show redundancy interfaces

Redundancy Management IP Address.............. 9.4.120.5
Peer Redundancy Management IP Address............ 9.4.120.3
Redundancy Port IP Address..................... 169.254.120.5
Peer Redundancy Port IP Address................ 169.254.120.3
Peer Service Port IP Address................... 10.104.175.189
```

show redundancy latency

管理ゲートウェイとピア冗長管理IPアドレスに到達するための平均遅延を表示するには、**show redundancy latency** コマンドを使用します。

show redundancy latency

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、管理ゲートウェイとピア冗長管理IPアドレスに到達するための平均遅延時間を表示する例を示します。

```
(Cisco Controller) >show redundancy latency

Network Latencies (RTT) for the Peer Reachability on the Redundancy Port in micro seconds
 for the past 10 intervals
Peer Reachability Latency[ 1 ]                  : 524 usecs
Peer Reachability Latency[ 2 ]                  : 524 usecs
Peer Reachability Latency[ 3 ]                  : 522 usecs
Peer Reachability Latency[ 4 ]                  : 526 usecs
Peer Reachability Latency[ 5 ]                  : 524 usecs
Peer Reachability Latency[ 6 ]                  : 524 usecs
Peer Reachability Latency[ 7 ]                  : 522 usecs
Peer Reachability Latency[ 8 ]                  : 522 usecs
Peer Reachability Latency[ 9 ]                  : 526 usecs
Peer Reachability Latency[ 10 ]                 : 523 usecs

Network Latencies (RTT) for the Management Gateway Reachability in micro seconds for the
 past 10 intervals
Gateway Reachability Latency[ 1 ]               : 1347 usecs
Gateway Reachability Latency[ 2 ]               : 2427 usecs
Gateway Reachability Latency[ 3 ]               : 1329 usecs
Gateway Reachability Latency[ 4 ]               : 2014 usecs
Gateway Reachability Latency[ 5 ]               : 2675 usecs
Gateway Reachability Latency[ 6 ]               : 731 usecs
Gateway Reachability Latency[ 7 ]               : 1882 usecs
Gateway Reachability Latency[ 8 ]               : 2853 usecs
Gateway Reachability Latency[ 9 ]               : 832 usecs
Gateway Reachability Latency[ 10 ]              : 3708 usecs
```

show redundancy mobilitymac

ピアとの通信に使用する高可用性（HA）モビリティの MAC アドレスを表示するには、 **show redundancy mobilitymac** コマンドを使用します。

show redundancy mobilitymac

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ピアとの通信に使用する HA モビリティの MAC アドレスを表示する例を示します。

```
(Cisco Controller) >show redundancy mobilitymac
         ff:ff:ff:ff:ff:ff
```

show redundancy peer-route summary

スタンバイ WLC に割り当てられているルートを表示するには、**show redundancy peer-route summary** コマンドを使用します。

show redundancy peer-route summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、スタンバイ WLC のすべての設定済みルートを表示する例を示します。

```
(Cisco Controller) >show redundancy peer-route summary
Number of Routes..................................... 1

Destination Network          Netmask              Gateway
-------------------    -------------------   -------------------
xxx.xxx.xxx.xxx           255.255.255.0       xxx.xxx.xxx.xxx
```

show redundancy peer-system statistics

スタンバイ WLCに関する統計情報を表示するには、 **show redundancy peer-system statistics** コマンドを使用します。

show redundancy peer-system statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.7	スタンバイ WLCのシリアル番号とファンのステータスが、コマンド出力に追加されました。
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

```
(Cisco Controller) >show redundancy peer-system statistics

        Peer System CPU statistics:Current CPU(s) load: 0%
       Individual CPU load: 0%/1%, 0%/0%, 0%/1%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%,
0%/0%, 0%/1%

       Peer System Memory Statistics:
       Total System Memory.............: 1027727360 bytes (980.18 MB)
       Used System Memory..............: 535404544 bytes (510.63 MB)
       Free System Memory..............: 492322816 bytes (469.54 MB)
       Bytes allocated from RTOS......: 5550080 bytes (5.29 MB)
       Chunks Free.....................: 7 bytes
       Number of mmapped regions......: 86
       Total space in mmapped regions.: 369500160 bytes (352.40 MB)
       Total allocated space..........: 4200328 bytes (4.00 MB)
       Total non-inuse space..........: 1349752 bytes (1.28 MB)
       Top-most releasable space......: 94664 bytes (92.44 KB)
       Total allocated (incl mmap)....: 375050240 bytes (357.70 MB)
       Total used (incl mmap).........: 373700488 bytes (356.41 MB)
       Total free (incl mmap).........: 1349752 bytes (1.28 MB)

       Peer system Power supply statistics:
       Power Supply 1..................................... Present, OK
       Power Supply 2..................................... Absent

       Serial Number..................................... XXXXXXXXX
       Fan Status.......................................... OK
```

show redundancy statistics

冗長マネージャの統計情報を表示するには、 **show redundancy statistics** コマンドを使用します。

show redundancy statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、異なる冗長性カウンタの統計情報を表示します。

ローカル物理ポート - コントローラの各物理ポート接続のステータス。1 はポートがアップしていることを示し、0 はポートがダウンしていることを示します。

ピア物理ポート - ピア コントローラの各物理ポート接続のステータス。1 はポートがアップしていることを示し、0 はポートがダウンしていることを示します。

次に、冗長マネージャの統計情報を表示する例を示します。

```
(Cisco Controller) >show redundancy statistics

        Redundancy Manager Statistics

        Keep Alive Request Send Counter          : 16
        Keep Alive Response Receive Counter      : 16

        Keep Alive Request Receive Counter       : 500322
        Keep Alive Response Send Counter         : 500322

        Ping Request to Default GW Counter       : 63360
        Ping Response from Default GW Counter    : 63360

        Ping Request to Peer Counter             : 12
        Ping Response from Peer Counter          : 3

        Keep Alive Loss Counter                  : 0
        Default GW Loss Counter                  : 0

        Local Physical Ports 1...8               : 10000000
        Peer  Physical Ports 1...8               : 10000000
```

show redundancy summary

冗長性の要約情報を表示するには、 **show redundancy summary** コマンドを使用します。

show redundancy summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、コントローラの冗長性の要約情報を表示する例を示します。

```
(Cisco Controller) >show redundancy summary
 Redundancy Mode = SSO DISABLED
     Local State = ACTIVE
      Peer State = N/A
            Unit = Primary
         Unit ID = 88:43:E1:7E:03:80
Redundancy State = N/A
    Mobility MAC = 88:43:E1:7E:03:80
Network Monitor = ENABLED
Link Encryption = DISABLED

 BulkSync Status = <Status>
Average Redundancy Peer Reachability Latency = 1390 usecs
Average Management Gateway Reachability Latency = 1165 usecs

Redundancy Management IP Address.............. 9.4.92.12
Peer Redundancy Management IP Address............ 9.4.92.14
Redundancy Port IP Address..................... 169.254.92.12
Peer Redundancy Port IP Address................ 169.254.92.14
```

show redundancy timers

冗長マネージャ タイマーの詳細を表示するには、 **show redundancy timers** コマンドを使用します。

show redundancy timers

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、冗長マネージャ タイマーの詳細を表示する例を示します。

```
(Cisco Controller) >show redundancy timers

          Keep Alive Timer         : 100 msecs

          Peer Search Timer        : 120 secs
```

show remote-lan

リモート LAN 設定に関する情報を表示するには、**show remote-lan** コマンドを使用します。

show remote-lan { **summary** | *remote-lan-id* }

構文の説明

summary	すべてのリモートLANのサマリーを表示します。
remote-lan-id	リモート LAN の識別子。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのリモート LAN のサマリーを表示する例を示します。

```
(Cisco Controller) >show remote-lan summary
Number of Remote LANS.............................. 2
RLAN ID  RLAN Profile Name                        Status    Interface Name
-------  -------------------------------------  --------  --------------------
2        remote                                 Disabled  management
8        test                                   Disabled  management
```

次に、*remote-lan-id* 2 を使用してリモート LAN に関する設定情報を表示する例を示します。

```
(Cisco Controller) >show remote-lan 2
Remote LAN Identifier.............................. 2
Profile Name....................................... remote
Status............................................. Disabled
MAC Filtering...................................... Disabled
AAA Policy Override................................ Disabled
Network Admission Control
  Radius-NAC State................................. Disabled
  SNMP-NAC State................................... Disabled
  Quarantine VLAN.................................. 0
Maximum number of Associated Clients.............. 0
Number of Active Clients........................... 0
Exclusionlist...................................... Disabled
Session Timeout.................................... Infinity
CHD per Remote LAN................................. Enabled
Webauth DHCP exclusion............................. Disabled
Interface.......................................... management
Remote LAN ACL..................................... unconfigured
DHCP Server........................................ Default
DHCP Address Assignment Required................... Disabled
Static IP client tunneling......................... Disabled
Radius Servers
   Authentication.................................. Global Servers
   Accounting...................................... Global Servers
```

```
   Dynamic Interface.............................. Disabled
Security
   Web Based Authentication....................... Enabled
        ACL.......................................... Unconfigured
        Web Authentication server precedence:
        1.............................................. local
        2.............................................. radius
        3.............................................. ldap
   Web-Passthrough................................ Disabled
   Conditional Web Redirect....................... Disabled
   Splash-Page Web Redirect....................... Disabled
```

show reset

スケジュールされたシステム リセット パラメータを表示するには、**show reset** コマンドを使用します。

show reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、スケジュールされたシステム リセット パラメータを表示する例を示します。

```
> show reset
System reset is scheduled for Mar 27 01 :01 :01 2010
Current local time and date is Mar 24 02:57:44 2010
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

関連コマンド

reset system at

reset system in

reset system cancel

reset system notify-time

show rfid client

クライアントとしてコントローラに関連付けられている無線周波数 ID（RFID）タグを表示するには、**show rfid client** コマンドを使用します。

show rfid client

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

使用上のガイドライン

RFID タグがクライアント モードではない場合、上記のフィールドは空白になります。

次に、クライアントとしてコントローラに関連付けられている RFID タグを表示する例を示します。

```
> show rfid client
------------------  -------- --------- ----------------- ------ ----------------
                                  Heard
   RFID Mac              VENDOR   Sec Ago    Associated AP    Chnl    Client State
------------------  -------- --------- ----------------- ------ ----------------
00:14:7e:00:0b:b1     Pango           35      AP0019.e75c.fef4     1          Probing
```

関連コマンド

config rfid status

config rfid timeout

show rfid config

show rfid detail

show rfid summary

show rfid config

現在の無線周波数 ID（RFID）構成設定を表示するには、**show rfid config** コマンドを使用します。

show rfid config

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、現在の RFID の設定情報を表示する例を示します。

```
> show rfid config
RFID Tag Data Collection ............................. Enabled
RFID Tag Auto-Timeout ................................ Enabled
RFID Client Data Collection .......................... Disabled
RFID Data Timeout .................................... 200 seconds
```

関連コマンド

config rfid status

config rfid timeout

show rfid client

show rfid detail

show rfid summary

show rfid detail

指定されたタグの詳細な無線周波数 ID（RFID）情報を表示するには、**show rfid detail** コマンドを使用します。

show rfid detail *mac_address*

構文の説明

mac_address	RFID タグの MAC アドレス。

コマンド デフォルト

なし。

次に、RFID の詳細情報を表示する例を示します。

```
> show rfid detail 00:12:b8:00:20:52
RFID address..................................... 00:12:b8:00:20:52
Vendor........................................... G2
Last Heard....................................... 51 seconds ago
Packets Received................................. 2
Bytes Received................................... 324
Cisco Type.....................................
Content Header
==================
Version.......................................... 0
Tx Power......................................... 12 dBm
Channel.......................................... 1
Reg Class........................................ 12
Burst Length..................................... 1
CCX Payload
===========
Last Sequence Control............................ 0
Payload length................................... 127
Last Sequence Control............................ 0
Payload length................................... 127
Payload Data Hex Dump
01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff
7f ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
50 ba 5b 97 27 80 00 67 00 01 03 05 01 42 34 00
00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
05 04 42 96 00 00 03 05 05 00 00 00 55 03 05 06
42 be 00 00 03 02 07 05 03 12 08 10 00 01 02 03
04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 03 0d 09 03
08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03
Nearby AP Statistics:
lap1242-2(slot 0, chan 1) 50 seconds ag.... -76 dBm
lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm
```

関連コマンド

config rfid status

config rfid timeout

show rfid config

show rfid client

show rfid summary

show rfid summary

指定されたタグの無線周波数ID（RFID）情報の要約を表示するには、**show rfid summary** コマンドを使用します。

show rfid summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、RFID 情報の要約を表示する例を示します。

```
> show rfid summary
Total Number of RFID   : 5
----------------- -------- ------------------ ------ --------------------
     RFID ID      VENDOR       Closest AP      RSSI  Time Since Last Heard
----------------- -------- ------------------ ------ --------------------
00:04:f1:00:00:04 Wherenet ap:1120             -51      858 seconds ago
00:0c:cc:5c:06:d3 Aerosct  ap:1120             -51       68 seconds ago
00:0c:cc:5c:08:45 Aerosct  AP_1130             -54      477 seconds ago
00:0c:cc:5c:08:4b Aerosct  wolverine           -54      332 seconds ago
00:0c:cc:5c:08:52 Aerosct  ap:1120             -51      699 seconds ago
```

関連コマンド

config rfid status

config rfid timeout

show rfid client

show rfid detail

show rfid config

show rf-profile summary

コントローラの RF プロファイルの要約を表示するには、**show rf-profile summary** コマンドを使用します。

show rf-profile summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show rf-profile summary** コマンドの出力を示します。

```
(Cisco Controller) >show rf-profile summary
Number of RF Profiles.......................... 2
Out Of Box State............................... Disabled
RF Profile Name            Band     Description                Applied
-------------------------  -------  -------------------------  -------
T1a                        5 GHz    <none>                     No
T1b                        2.4 GHz  <none>                     No
```

show rf-profile details

Cisco Wireless LAN Controller の RF プロファイルの詳細を表示するには、**show rf-profile details** コマンドを使用します。

show rf-profile details *rf-profile-name*

構文の説明

rf-profile-name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	出力は、Rx SOP しきい値を含むように更新されました。

次に、**show rf-profile details** コマンドの出力を示します。

```
(Cisco Controller) >show rf-profile details T1a
Description..................................... <none>
Radio policy.................................... 5 GHz
Transmit Power Threshold v1..................... -70 dBm
Transmit Power Threshold v2..................... -67 dBm
Min Transmit Power.............................. -10 dBm
Max Transmit Power.............................. 30 dBm
Rx Sop Threshold................................ Medium
802.11a Operational Rates
    802.11a 6M Rate............................. Mandatory
    802.11a 9M Rate............................. Supported
    802.11a 12M Rate............................ Mandatory
    802.11a 18M Rate............................ Supported
    802.11a 24M Rate............................ Mandatory
    802.11a 36M Rate............................ Supported
    802.11a 48M Rate............................ Supported
    802.11a 54M Rate............................ Supported
Max Clients..................................... 200
Client Trap Threshold........................... 50
Multicast Data Rate............................. 0
Rx Sop Threshold................................ 0 dBm
Cca Threshold................................... 0 dBm
Slot Admin State:............................... Enabled
Band Select Probe Response...................... Disabled
Band Select Cycle Count......................... 2 cycles
Band Select Cycle Threshold..................... 200 milliseconds
Band Select Expire Suppression.................. 20 seconds
Band Select Expire Dual Band.................... 60 seconds
Band Select Client Rssi......................... -80 dBm
Load Balancing Denial........................... 3 count
Load Balancing Window........................... 5 clients
Coverage Data................................... -80 dBm
Coverage Voice.................................. -80 dBm
Coverage Exception.............................. 3 clients
Coverage Level.................................. 25 %
```

show rogue adhoc custom summary

カスタムのアドホックの不正なアクセス ポイントに関する情報を表示するには、**show rogue adhoc custom summary** コマンドを使用します。

show rogue adhoc custom summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、カスタムのアドホックの不正なアクセス ポイントの詳細を表示する例を示します。

```
(Cisco Controller) > show rogue adhoc custom summary
Number of Adhocs.............................0

MAC Address         State               # APs # Clients Last Heard
-----------------  ------------------ ----- ---------
-----------------------
```

関連コマンド

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc malicious summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc detailed

Cisco ワイヤレス LAN コントローラによって検出されたアドホックの不正なアクセス ポイントの詳細を表示するには、**show rogue adhoc client detailed** コマンドを使用します。

show rogue adhoc detailed *MAC_address*

構文の説明

MAC_address	アドホックの不正なアクセスポイントのMACアドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、アドホックの不正なアクセス ポイントの MAC アドレスの詳細情報を表示する例を示します。

```
(Cisco Controller) > show rogue adhoc client detailed 02:61:ce:8e:a8:8c
Adhoc Rogue MAC address..................... 02:61:ce:8e:a8:8c
Adhoc Rogue BSSID........................... 02:61:ce:8e:a8:8c
State....................................... Alert
First Time Adhoc Rogue was Reported.............. Tue Dec 11 20:45:45
2007
Last Time Adhoc Rogue was Reported.............. Tue Dec 11 20:45:45
2007
Reported By
AP 1
MAC Address............................. 00:14:1b:58:4a:e0
Name.................................... AP0014.1ced.2a60
Radio Type.............................. 802.11b
SSID.................................... rf4k3ap
Channel................................. 3
RSSI.................................... -56 dBm
SNR..................................... 15 dB
Encryption.............................. Disabled
ShortPreamble........................... Disabled
WPA Support............................. Disabled
Last reported by this AP.............. Tue Dec 11 20:45:45 2007
```

関連コマンド

config rogue adhoc

show rogue ignore-list

show rogue rule summary

show rogue rule detailed

config rogue rule

show rogue adhoc summary

show rogue adhoc friendly summary

危険性のないアドホックの不正なアクセス ポイントに関する情報を表示するには、**show rogue adhoc friendly summary** コマンドを使用します。

show rogue adhoc friendly summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、危険性のないアドホックの不正なアクセス ポイントの詳細を表示する例を示します。

```
(Cisco Controller) > show rogue adhoc friendly summary

Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

関連コマンド

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc malicious summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc malicious summary

悪意のあるアドホックの不正なアクセス ポイントに関する情報を表示するには、**show rogue adhoc malicious summary** コマンドを使用します。

show rogue adhoc malicious summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、悪意のあるアドホックの不正なアクセス ポイントの詳細を表示する例を示します。

```
(Cisco Controller) > show rogue adhoc malicious summary
Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------ -----  ---------
-----------------------
```

関連コマンド

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc unclassified summary

未分類のアドホックの不正なアクセス ポイントに関する情報を表示するには、**show rogue adhoc unclassified summary** コマンドを使用します。

show rogue adhoc unclassified summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、未分類のアドホックの不正なアクセス ポイントの詳細を表示する例を示します。

```
(Cisco Controller) > show rogue adhoc unclassified summary

Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

関連コマンド

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc malicious summary

config rogue adhoc

show rogue adhoc summary

Cisco Wireless LAN Controller によって検出されたアドホックの不正なアクセス ポイントのサマリーを表示するには、**show rogue adhoc summary** コマンドを使用します。

show rogue adhoc summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべてのアドホックの不正なアクセス ポイントのサマリーを表示する例を示します。

```
(Cisco Controller) > show rogue adhoc summary
Detect and report Ad-Hoc Networks..... Enabled
Client MAC Address   Adhoc BSSID    State  # APs       Last Heard
------------------   -----------    -----    ---       -------
xx:xx:xx:xx:xx:xx    super          Alert    1         Sat Aug  9
21:12:50 2004
xx:xx:xx:xx:xx:xx                   Alert    1         Aug  9 21:12:50
 2003
xx:xx:xx:xx:xx:xx                   Alert    1         Sat Aug  9
21:10:50 2003
```

関連コマンド

config rogue adhoc

show rogue ignore-list

show rogue rule summary

show rogue rule detailed

config rogue rule

show rogue adhoc detailed

show rogue ap clients

Cisco ワイヤレス LAN コントローラによって検出された不正なアクセス ポイント クライアントの詳細を表示するには、**show rogue ap clients** コマンドを使用します。

show rogue ap clients *ap_mac_address*

構文の説明

ap_mac_address	不正なアクセス ポイントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、不正なアクセス ポイント クライアントの詳細を表示する例を示します。

```
(Cisco Controller) > show rogue ap clients xx:xx:xx:xx:xx:xx
MAC Address State # APs Last Heard
----------------- ------------------ ----- -------------------------
00:bb:cd:12:ab:ff Alert 1 Fri Nov 30 11:26:23 2007
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap custom summary

カスタムのアドホックの不正なアクセス ポイントに関する情報を表示するには、**show rogue ap custom summary** コマンドを使用します。

show rogue ap custom summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、カスタムのアドホックの不正なアクセス ポイントの詳細を表示する例を示します。

```
(Cisco Controller) > show rogue ap custom summary

Number of APs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------ -----  ---------
-----------------------
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap detailed

Cisco ワイヤレス LAN コントローラによって検出された不正なアクセス ポイントの詳細を表示するには、**show rogue-ap detailed** コマンドを使用します。

show rogue ap detailed *ap_mac_address*

構文の説明

ap_mac_address	不正なアクセス ポイントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、不正なアクセス ポイントの詳細情報を表示する例を示します。

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..................................... 00:0b:85:63:d1:94
Is Rogue on Wired Network....................... No
Classification.................................. Unclassified
State........................................... Alert
First Time Rogue was Reported................... Fri Nov 30 11:24:56
2007
Last Time Rogue was Reported.................... Fri Nov 30 11:24:56
2007
Reported By
AP 1
MAC Address.............................. 00:12:44:bb:25:d0
Name..................................... flexconnect
Radio Type............................... 802.11g
SSID..................................... edu-eap
Channel.................................. 6
RSSI..................................... -61 dBm
SNR...................................... -1 dB
Encryption............................... Enabled
ShortPreamble............................ Enabled
WPA Support.............................. Disabled
Last reported by this AP.............. Fri Nov 30 11:24:56 2007
```

次に、不正なアクセス ポイントの詳細情報をカスタマイズされた分類によって表示する例を示します。

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..................................... 00:17:0f:34:48:a0
Is Rogue on Wired Network....................... No
```

```
Classification.................................. custom
Severity Score ................................. 1
Class Name.....................................VeryMalicious
Class Change by................................. Rogue Rule
Classified at .................................. -60 dBm
Classified by................................... c4:0a:cb:a1:18:80

State........................................... Contained
State change by................................. Rogue Rule
First Time Rogue was Reported................... Mon Jun  4 10:31:18
2012
Last Time Rogue was Reported.................... Mon Jun  4 10:31:18
2012
Reported By
    AP 1
        MAC Address............................. c4:0a:cb:a1:18:80
        Name.................................... SHIELD-3600-2027
        Radio Type.............................. 802.11g
        SSID.................................... sri
        Channel................................. 11
        RSSI.................................... -87 dBm
        SNR..................................... 4 dB
        Encryption.............................. Enabled
        ShortPreamble........................... Enabled
        WPA Support............................. Enabled
        Last reported by this AP................ Mon Jun  4 10:31:18
2012
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap friendly summary

コントローラによって検出された危険性のない不正なアクセス ポイントを一覧表示するには、**show rogue ap friendly summary** コマンドを使用します。

show rogue ap friendly summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての危険性のない不正なアクセス ポイントのサマリーを表示する例を示します。

```
(Cisco Controller) > show rogue ap friendly summary
Number of APs.................................... 1
MAC Address       State     # APs  # Clients Last Heard
----------------- ----------------- ----- ---------
---------------------------
XX:XX:XX:XX:XX:XX Internal    1   0  Tue Nov 27 13:52:04 2007
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap malicious summary

コントローラによって検出された悪意のある不正なアクセス ポイントを一覧表示するには、**show rogue ap malicious summary** コマンドを使用します。

show rogue ap malicious summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての悪意のある不正なアクセス ポイントのサマリーを表示する例を示します。

```
(Cisco Controller) > show rogue ap malicious summary
Number of APs.................................... 2
MAC Address       State     # APs  # Clients Last Heard
----------------- ----------------- ----- ---------
---------------------------
XX:XX:XX:XX:XX:XX Alert           1   0  Tue Nov 27 13:52:04 2007
XX:XX:XX:XX:XX:XX Alert           1   0  Tue Nov 27 13:52:04 2007
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap summary

Cisco ワイヤレス LAN コントローラによって検出された不正なアクセス ポイントのサマリーを表示するには、**show rogue-ap summary** コマンドを使用します。

show rogue ap summary{ssid | channel}

構文の説明

ssid	不正なアクセス ポイントの特定のユーザに設定された SSID を表示します。
channel	不正なアクセス ポイントの特定のユーザに設定された無線タイプおよびチャネルを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	新しいキーワード **SSID** と **channel** が追加されました。

次に、すべての不正なアクセス ポイントのサマリーを表示する例を示します。

```
(Cisco Controller) > show rogue ap summary

Rogue Location Discovery Protocol.................  Disabled
Rogue ap timeout..................................  1200
Rogue on wire Auto-Contain....................... Disabled
Rogue using our SSID Auto-Contain................ Disabled
Valid client on rogue AP Auto-Contain............ Disabled
Rogue AP timeout................................. 1200
Rogue Detection Report Interval.................. 10
Rogue Detection Min Rssi......................... -128
Rogue Detection Transient Interval............... 0
Rogue Detection Client Num Thershold.............. 0
Total Rogues(AP+Ad-hoc) supported................ 2000
Total Rogues classified.......................... 729

MAC Address        Classification     # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
xx:xx:xx:xx:xx:xx  friendly           1     0         Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 19:00:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 18:57:11 2005
```

次に、すべての不正なアクセス ポイントのサマリーと拡張パラメータとしての SSID を表示する例を示します。

```
(Cisco Controller) > show rogue ap summary ssid

MAC Address        Class              State      SSID  Security
-------------------------------------------------------------------------------------

xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   Open
xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   Open
xx:xx:xx:xx:xx:xx  Pending            Pending     xxx   Open
xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   WEP/WPA
```

次に、すべての不正なアクセス ポイントのサマリーと拡張パラメータとしてのチャネルを表示する例を示します。

```
(Cisco Controller) > show rogue ap summary channel

MAC Address        Class              State  Det RadioType    Channel RSSIlast/Max)
-------------------------------------------------------------------------------------

xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11g           11    -53 / -48
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11g           11    -53 / -48
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
```

次に、すべての不正なアクセス ポイントのサマリーと拡張パラメータとしての SSID とチャネルの両方を表示する例を示します。

```
(Cisco Controller) > show rogue ap summary ssid channel

MAC Address        Class        State    SSID                  Security  Det RadioType
Channel  RSSI(last/Max)
-------------------------------------------------------------------------------------
xx:xx:xx:xx:xx:xx  Unclassified  Alert   dd                    WEP/WPA     802.11n5G
  56    -73 / -62
xx:xx:xx:xx:xx:xx  Unclassified  Alert   SSID IS HIDDEN        Open        802.11a
  149   -68 / -66
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan16                WEP/WPA     802.11n5G
  149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan15                WEP/WPA     802.11n5G
  149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan14                WEP/WPA     802.11n5G
  149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan13                WEP/WPA     802.11n5G
  149   -71 / -70
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan12                WEP/WPA     802.11n5G
  149   -71 / -71
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap unclassified summary

コントローラによって検出された未分類の不正なアクセスポイントを一覧表示するには、**show rogue ap unclassified summary** コマンドを使用します。

show rogue ap unclassified summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、すべての未分類の不正なアクセス ポイントのリストを表示する例を示します。

```
(Cisco Controller) > show rogue ap unclassified summary
Number of APs..................................... 164
MAC Address       State  # APs # Clients Last Heard
----------------- ------------ ----- --------- ---------------
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:12:52 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:29:01 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:26:23 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:26:23 2007
```

show rogue auto-contain

不正の自動阻止に関する情報を表示するには、**show rogue auto-contain** コマンドを使用します。

show rogue auto-contain

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、不正の自動阻止に関する情報を表示する例を示します。

```
(Cisco Controller) > show rogue auto-contain
Containment Level.............................. 3
monitor_ap_only................................ false
```

関連コマンド

config rogue adhoc

config rogue auto-contain level

show rogue client detailed

Cisco ワイヤレス LAN コントローラによって検出された不正なクライアントの詳細を表示するには、**show rogue client detailed** コマンドを使用します。

show rogue client detailed *Rogue_AP MAC_address*

構文の説明

Rogue_AP	不正 AP のアドレス。
MAC_address	不正なクライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.1	*Rogue_AP* パラメータが **show rogue client detailed** コマンドに追加されました。

次に、不正なクライアントの詳細情報を表示する例を示します。

```
(Cisco Controller) > show rogue client detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..................................... 00:0b:85:23:ea:d1
State........................................... Alert
First Time Rogue was Reported................... Mon Dec 3 21:50:36 2007
Last Time Rogue was Reported.................... Mon Dec 3 21:50:36 2007
Rogue Client IP address......................... Not known
Reported By
AP 1
MAC Address.............................. 00:15:c7:82:b6:b0
Name..................................... AP0016.47b2.31ea
Radio Type............................... 802.11a
RSSI..................................... -71 dBm
SNR...................................... 23 dB
Channel.................................. 149
Last reported by this AP.............. Mon Dec 3 21:50:36 2007
```

関連コマンド

show rogue client summary

show rogue ignore-list

config rogue rule client

config rogue rule

show rogue client summary

Cisco ワイヤレス LAN コントローラによって検出された不正なクライアントのサマリーを表示するには、**show rogue client summary** コマンドを使用します。

show rogue client summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、すべての不正なクライアントのリストを表示する例を示します。

```
(Cisco Controller) > show rogue client summary
Validate rogue clients against AAA.............. Disabled
Total Rogue Clients supported..................... 2500
Total Rogue Clients present..................... 3
MAC Address        State              # APs Last Heard
-----------------  -----------------  ----- ----------------------
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 18:57:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:12:08 2005
```

関連コマンド

show rogue client detailed

show rogue ignore-list

config rogue client

config rogue rule

show rogue ignore-list

無視するように設定されている不正なアクセスポイントのリストを表示するには、**show rogue ignore-list** コマンドを使用します。

show rogue ignore-list

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、無視するように設定されているすべての不正なアクセスポイントのリストを表示する例を示します。

```
(Cisco Controller) > show rogue ignore-list

MAC Address
------------------
xx:xx:xx:xx:xx:xx
```

関連コマンド

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue ignore-list

show rogue rule summary

show rogue client summary

show rogue ap unclassified summary

show rogue ap malicious summary

show rogue ap friendly summary

config rogue client

show rogue ap summary

show rogue ap clients

show rogue ap detailed

config rogue rule

show rogue rule detailed

特定の不正な分類ルールの詳細情報を表示するには、**show rogue rule detailed** コマンドを使用します。

show rogue rule detailed *rule_name*

構文の説明

rule_name	不正な分類ルールの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、特定の不正な分類ルールの詳細情報を表示する例を示します。

```
(Cisco Controller) > show rogue rule detailed Rule2
Priority..................................... 2
Rule Name.................................... Rule2
State........................................ Enabled
Type......................................... Malicious
Severity Score............................... 1
Class Name................................... Very_Malicious
Notify....................................... All
State ....................................... Contain
Match Operation.............................. Any
Hit Count.................................... 352
Total Conditions............................. 2
Condition 1
    type..................................... Client-count
    value.................................... 10
Condition 2
    type..................................... Duration
    value (seconds).......................... 2000
Condition 3
    type..................................... Managed-ssid
    value.................................... Enabled
Condition 4
    type..................................... No-encryption
    value.................................... Enabled
Condition 5
    type..................................... Rssi
    value (dBm).............................. -50
Condition 6
    type..................................... Ssid
    SSID Count............................... 1
    SSID 1................................... test
```

関連コマンド

config rogue rule

show rogue ignore-list

show rogue rule summary

show rogue rule summary

コントローラに設定されている不正な分類ルールを表示するには、**show rogue rule summary** コマンドを使用します。

show rogue rule summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、コントローラに設定されているすべての不正なルールのリストを表示する例を示します。

```
(Cisco Controller) > show rogue rule summary
Priority Rule Name                State    Type          Match Hit Count
-------- ------------------------ -------- ------------- ----- ---------
1        mtest                     Enabled  Malicious     All   0
2        asdfasdf                  Enabled  Malicious     All   0
```

次に、コントローラに設定されているすべての不正なルールのリストを表示する例を示します。

```
(Cisco Controller) > show rogue rule summary
Priority         Rule Name                  Rule state Class Type
Notify   State    Match Hit Count
-------- -------------------------------- ----------- -----------
-------- -------- ------ ---------
1        rule2                            Enabled    Friendly     Global
   Alert    All    234
2        rule1                            Enabled    Custom       Global
   Alert    All    0
```

関連コマンド

config rogue rule

show rogue ignore-list

show rogue rule detailed

show route kernel

カーネルのルート キャッシュ情報を表示するには、**show route kernel** コマンドを使用します。

show route kernel

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、カーネルのルート キャッシュ情報を表示する例を示します。

```
> show route kernel
Iface  Destination  Gateway   Flags    RefCnt Use  Metric   Mask   MTU   Window   IRTT
dtl0    14010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    28282800    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    34010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
eth0    02020200    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    33010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    0A010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    32010100    00000000  0001      0     0     0    FFFFFF00  0      0        0
dtl0    0A000000    0202020A  0003      0     0     0    FF000000  0      0        0
lo      7F000000    00000000  0001      0     0     0    FF000000  0      0        0
dtl0    00000000    0A010109  0003      0     0     0    00000000  0      0        0
```

関連コマンド

clear ap

debug arp

show arp kernel

config route add

config route delete

show route summary

Cisco ワイヤレス LAN コントローラ サービス ポートに割り当てられているルートを表示するには、**show route summary** コマンドを使用します。

show route summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、設定されたすべてのルートを表示する例を示します。

```
> show route summary
Number of Routes.............................. 1
Destination Network          Genmask               Gateway
-------------------    -------------------   -------------------
xxx.xxx.xxx.xxx        255.255.255.0         xxx.xxx.xxx.xxx
```

関連コマンド

config route

show rules

アクティブな内部ファイアウォール ルールを表示するには、**show rules** コマンドを使用します。

show rules

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、アクティブな内部ファイアウォール ルールを表示する例を示します。

```
(Cisco Controller) > show rules
-------------------------------------------------------
Rule ID.............: 3
Ref count...........: 0
Precedence..........: 99999999
Flags...............: 00000001 ( PASS )
Source IP range:
        (Local stack)
Destination IP range:
        (Local stack)
-------------------------------------------------------
Rule ID.............: 25
Ref count...........: 0
Precedence..........: 99999999
Flags...............: 00000001 ( PASS )
Service Info
        Service name........: GDB
        Protocol............: 6
        Source port low.....: 0
        Source port high....: 0
        Dest port low.......: 1000
        Dest port high......: 1000
Source IP range:
IP High.............: 0.0.0.0
        Interface...........: ANY
Destination IP range:
        (Local stack)
-------------------------------------------------------
```

show run-config

現在の Cisco コントローラの設定の包括的なビューを表示するには、**show run-config all** コマンドを使用します。

show run-config {**all** | **commands**} [**no-ap** | **commands**]

構文の説明

all	show run-config の下のすべてのコマンドを表示します。
no-ap	（任意）アクセスポイント設定を除外します。
commands	（任意）コントローラにユーザが設定したコマンドを一覧表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.2	このコマンドが追加されました。

使用上のガイドライン

次のコマンドが **show running-config** コマンドに置き換えられました。

show run-config all コマンドで表示されるのは、ユーザが設定した値だけです。システムにより設定されたデフォルト値は表示されません。

次に、**show run-config all** コマンドの出力例を示します。

```
(Cisco Controller) > show run-config all
Press Enter to continue...
System Inventory
Switch Description.............................. Cisco Controller
Machine Model...................................
Serial Number................................... FLS0923003B
Burned-in MAC Address........................... xx:xx:xx:xx:xx:xx
Crypto Accelerator 1............................ Absent
Crypto Accelerator 2............................ Absent
Power Supply 1.................................. Absent
Power Supply 2.................................. Present, OK
Press Enter to continue Or <Ctl Z> to abort...
```

show run-config startup-commands

現在の Cisco ワイヤレス LAN コントローラの設定の包括的なビューを表示するには、**showrun-configstartup-commands** コマンドを使用します。

show run-configstartup-commands

構文の説明

run-config	実行中のコンフィギュレーション コマンドを表示します。
startup-commands	ワイヤレス LAN コントローラで設定されているスタートアップ コマンドのリストを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	

使用上のガイドライン

無線 LAN コントローラのコンフィギュレーション コマンドは、転送アップロード プロセスを使用して TFTP または NCS サーバにアップロードされます。**show run-config startup-commands** コマンドにより、無線 LAN コントローラは実行中のコンフィギュレーションを CLI 形式で生成することができます。生成された設定コマンドは、ネットワークを復元するためのバックアップ コンフィギュレーションとして使用できます。

例

次に、**show run-config startup-commands** コマンドの出力例を示します。

show run-config startup-commands

```
(Cisco Controller) >show run-config
  startup-commands

(Cisco Controller) >show run-config startup-commands

This may take some time.
Are you sure you want to proceed? (y/N) y


config location expiry tags 5
config mdns profile service add default-mdns-profile AirPrint
config mdns profile service add default-mdns-profile AirTunes
config mdns profile service add default-mdns-profile AppleTV
config mdns profile service add default-mdns-profile HP_Photosmart_Printer_1
config mdns profile service add default-mdns-profile HP_Photosmart_Printer_2
config mdns profile service add default-mdns-profile Printer
config mdns profile create default-
```

show serial

シリアル（コンソール）ポート設定を表示するには、**show serial** コマンドを使用します。

show serial

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ポート設定のボー レート、文字、フロー制御、ストップ ビット、パリティ タイプのデフォルト値は、9600、8、off、1、none です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、EIA-232 パラメータおよびシリアル ポートの非アクティブ タイムアウトを表示する例を示します。

```
(Cisco Controller) > show serial
Serial Port Login Timeout (minutes)..... 45
Baud Rate............................... 9600
Character Size.......................... 8
Flow Control:........................... Disable
Stop Bits............................... 1
Parity Type:............................ none
```

show sessions

コンソールポートのログインタイムアウトおよび同時コマンドラインインターフェイス（CLI）セッションの最大数を表示するには、**show sessions** コマンドを使用します。

show sessions

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

5 分、5 セッション。

次に、CLI セッションの設定を表示する例を示します。

```
> show sessions
CLI Login Timeout (minutes)..... 0
Maximum Number of CLI Sessions..... 5
```

この応答は、CLI セッションがタイムアウトすることはなく、Cisco ワイヤレス LAN コントローラは最大で5つの同時CLIセッションをホストできることを示しています。

関連コマンド

config sessions maxsessions

config sessions timeout

show snmpcommunity

Simple Network Management Protocol（SNMP）コミュニティ エントリを表示するには、**show snmpcommunity** コマンドを使用します。

show snmpcommunity

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、SNMP コミュニティ エントリを表示する例を示します。

```
> show snmpcommunity
SNMP Community Name Client IP Address Client IP Mask    Access Mode Status
------------------- ------------------ ----------------- ----------- --------
public              0.0.0.0            0.0.0.0           Read Only   Enable
**********          0.0.0.0            0.0.0.0           Read/Write  Enable
```

関連コマンド

config snmp community accessmode

config snmp community create

config snmp community delete

config snmp community ipaddr

config snmp community mode

config snmp syscontact

show snmpengineID

SNMP エンジン ID を表示するには、**show snmpengineID** コマンドを使用します。

show snmpengineID

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、SNMP エンジン ID を表示する例を示します。

```
> show snmpengineID
SNMP EngineId... ffffffffffff
```

関連コマンド

config snmp engineID

show snmptrap

Cisco ワイヤレス LAN コントローラの Simple Network Management Protocol（SNMP）のトラップ レシーバとそれらのステータスを表示するには、**show snmptrap** コマンドを使用します。

show snmptrap

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、SNMP トラップ レシーバとそれらのステータスを表示する例を示します。

```
> show snmptrap
SNMP Trap Receiver Name    IP Address        Status
-------------------------  ----------------- --------
xxx.xxx.xxx.xxx            xxx.xxx.xxx.xxx   Enable
```

show snmpv3user

Simple Network Management Protocol（SNMP）バージョン 3 の設定を表示するには、**show snmpv3user** コマンドを使用します。

show snmpv3user

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、SNMP バージョン 3 の設定情報を表示する例を示します。

```
> show snmpv3user
SNMP v3 username    AccessMode  Authentication Encryption
------------------- ----------- -------------- ----------
default              Read/Write  HMAC-SHA       CFB-AES
```

関連コマンド

config snmp v3user create

config snmp v3user delete

show snmpversion

コントローラ上でどのバージョンの簡易ネットワーク管理プロトコル（SNMP）が有効または無効になっているかを表示するには、**show snmpversion** コマンドを使用します。

show snmpversion

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

イネーブル

次に、SNMP v1/v2/v3 ステータスを表示する例を示します。

```
> show snmpversion
SNMP v1  Mode..................................... Disable
SNMP v2c Mode..................................... Enable
SNMP v3  Mode..................................... Enable
```

関連コマンド

config snmp version

show spanningtree port

Cisco ワイヤレス LAN コントローラのスパニングツリー ポート設定を表示するには、**show spanningtree port** コマンドを使用します。

show spanningtree port *port*

構文の説明

port	物理ポート番号： • Cisco 2100 シリーズ ワイヤレス LAN コントローラでは 1 ～ 4。 • Cisco 4402 シリーズ ワイヤレス LAN コントローラでは 1 または 2。 • Cisco 4404 シリーズ ワイヤレス LAN コントローラでは 1 ～ 4。

コマンド デフォルト

SPT のデフォルト設定の出力値は、800C、Disabled、802.1D、128、100、Auto です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

Cisco 4400 シリーズ ワイヤレス LAN コントローラでポート冗長化が設定されている場合、Cisco 4400 シリーズ ワイヤレス LAN コントローラのすべてのポートに対してスパニングツリー プロトコル（STP）を無効にする必要があります。Cisco 4400 シリーズ ワイヤレス LAN コントローラに接続されているスイッチでは、STP を有効のままにしておくことができます。

（注） 一部の WLAN コントローラは、スパニングツリー機能をサポートしていません。

次に、ポート単位でスパニングツリー値を表示する例を示します。

```
(Cisco Controller) > show spanningtree port 3
STP Port ID..................................... 800C
STP Port State.................................. Disabled
STP Port Administrative Mode.................... 802.1D
STP Port Priority............................... 128
STP Port Path Cost.............................. 100
STP Port Path Cost Mode......................... Auto
```

show spanningtree switch

Cisco ワイヤレス LAN コントローラのネットワーク（DS ポート）スパニングツリー設定を表示するには、**show spanningtree switch** コマンドを使用します。

show spanningtree switch

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

一部の WLAN コントローラは、スパニングツリー機能をサポートしていません。

次に、スイッチ単位でスパニングツリー値を表示する例を示します。

```
(Cisco Controller) > show spanningtree switch
STP Specification..................... IEEE 802.1D
STP Base MAC Address.................. 00:0B:85:02:0D:20
Spanning Tree Algorithm............... Disable
STP Bridge Priority................... 32768
STP Bridge Max. Age (seconds)......... 20
STP Bridge Hello Time (seconds)....... 2
STP Bridge Forward Delay (seconds)..... 15
```

show stats port

物理ポートの送受信の統計情報を表示するには、**show stats port** コマンドを使用します。

show stats port {**detailed** *port* | **summary** *port*}

構文の説明

detailed	詳細なポート統計情報を表示します。
summary	ポート統計情報の要約を表示します。
port	物理ポート番号： • Cisco 2100 シリーズ ワイヤレス LAN コントローラでは 1 ～ 4。 • Cisco 4402 シリーズ ワイヤレス LAN コントローラでは 1 または 2。 • Cisco 4404 シリーズ ワイヤレス LAN コントローラでは 1 ～ 4。 • Cisco WLCM シリーズ ワイヤレス LAN コントローラでは 1。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ポート要約情報を表示する例を示します。

```
(Cisco Controller) > show stats port summary
Packets Received Without Error..................... 399958
Packets Received With Error........................ 0
Broadcast Packets Received......................... 8350
Packets Transmitted Without Error.................. 106060
Transmit Packets Errors............................ 0
Collisions Frames.................................. 0
Time Since Counters Last Cleared.................... 2 day 11 hr 16 min 23
sec
```

次に、詳細なポート情報を表示する例を示します。

```
(Cisco Controller) > show stats port detailed 1
PACKETS RECEIVED (OCTETS)
```

```
Total Bytes..................................... 267799881
64 byte pkts        :918281
65-127 byte pkts    :354016         128-255 byte pkts   :1283092
256-511 byte pkts   :8406           512-1023 byte pkts  :3006
1024-1518 byte pkts :1184           1519-1530 byte pkts :0
> 1530 byte pkts    :2
PACKETS RECEIVED SUCCESSFULLY
Total..................................... 2567987
Unicast Pkts  :2547844       Multicast Pkts:0          Broadcast
Pkts:20143
PACKETS RECEIVED WITH MAC ERRORS
Total..................................... 0
Jabbers   :0              Undersize :0              Alignment :0
FCS Errors:0              Overruns  :0
RECEIVED PACKETS NOT FORWARDED
Total..................................... 0
Local Traffic Frames:0              RX Pause Frames     :0
Unacceptable Frames :0              VLAN Membership     :0
VLAN Viable Discards:0              MulticastTree Viable:0
ReserveAddr Discards:0
CFI Discards        :0              Upstream Threshold  :0
PACKETS TRANSMITTED (OCTETS)
Total Bytes..................................... 353831
64 byte pkts        :0              65-127 byte pkts    :0
128-255 byte pkts   :0              256-511 byte pkts   :0
512-1023 byte pkts  :0              1024-1518 byte pkts :2
1519-1530 byte pkts :0              Max Info            :1522
PACKETS TRANSMITTED SUCCESSFULLY
Total..................................... 5875
Unicast Pkts  :5868           Multicast Pkts:0           Broadcast
Pkts:7
TRANSMIT ERRORS
Total Errors.................................... 0
FCS Error     :0          TX Oversized  :0          Underrun Error:0
TRANSMIT DISCARDS
Total Discards.................................. 0
Single Coll Frames  :0              Multiple Coll Frames:0
Excessive Coll Frame:0              Port Membership     :0
VLAN Viable Discards:0
PROTOCOL STATISTICS
BPDUs Received      :6              BPDUs Transmitted   :0
802.3x RX PauseFrame:0
Time Since Counters Last Cleared..... 2 day 0 hr 39 min 59
sec
```

show stats switch

ネットワーク（DS ポート）の送受信の統計情報を表示するには、**show stats switch** コマンドを使用します。

show stats switch {**detailed** | **summary**}

構文の説明

detailed	詳細なスイッチ統計情報を表示します。
summary	スイッチ統計情報の要約を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、スイッチ統計情報の要約を表示する例を示します。

```
(Cisco Controller) > show stats switch summary
Packets Received Without Error..................... 136410
Broadcast Packets Received..................... 18805
Packets Received With Error..................... 0
Packets Transmitted Without Error.............. 78002
Broadcast Packets Transmitted.................. 3340
Transmit Packet Errors......................... 2
Address Entries Currently In Use............... 26
VLAN Entries Currently In Use.................. 1
Time Since Counters Last Cleared............... 2 day 11 hr 22 min 17
sec
```

次に、詳細なスイッチ統計情報を表示する例を示します。

```
(Cisco Controller) > show stats switch detailed
RECEIVE
Octets..................................... 19351718
Total Pkts..................................... 183468
Unicast Pkts................................... 180230
Multicast Pkts................................. 3219
Broadcast Pkts................................. 19
Pkts Discarded................................. 0
TRANSMIT
Octets..................................... 354251
Total Pkts..................................... 5882
Unicast Pkts................................... 5875
Multicast Pkts................................. 0
```

```
Broadcast Pkts..................................... 7
Pkts Discarded..................................... 0
ADDRESS ENTRIES
Most Ever Used..................................... 1
Currently In Use................................... 1
VLAN ENTRIES
Maximum............................................ 128
Most Ever Used..................................... 1
Static In Use...................................... 1
Dynamic In Use..................................... 0
VLANs Deleted...................................... 0
Time Since Ctrs Last Cleared..................... 2 day 0 hr 43 min 22
 sec
```

show switchconfig

Cisco ワイヤレス LAN コントローラに適用するパラメータを表示するには、**show switchconfig** コマンドを使用します。

show switchconfig

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

イネーブル

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco ワイヤレス LAN コントローラに適用するパラメータを表示する例を示します。

```
(Cisco Controller) >> show switchconfig
802.3x Flow Control Mode..................... Disabled
FIPS prerequisite features................... Enabled
Boot Break................................... Enabled
secret obfuscation........................... Enabled
Strong Password Check Features:
         case-check ...........Disabled
         consecutive-check ....Disabled
         default-check .......Disabled
         username-check ......Disabled
```

関連コマンド

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig strong-pwd

config switchconfig flowcontrol

config switchconfig fips-prerequisite

show stats switch

show sysinfo

Cisco WLC の概要情報を表示するには、**show sysinfo** コマンドを使用します。

show sysinfo

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

show system iostat

CPU統計情報、デバイスの入出力統計情報、およびパーティションとシステムの詳細統計情報を表示するには、**show system iostat** コマンドを使用します。

show system iostat {**detail** | **summary**}

構文の説明

detail	CPU 統計情報、デバイスの入出力統計情報、およびパーティションとシステムの詳細統計情報を表示します。
summary	CPU 統計情報、デバイスの入出力統計情報、およびシステムのパーティションを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、**show system iostat summary** コマンドの出力例を示します。

```
(Cisco Controller) >show system iostat summary
 Linux 2.6.21_mvlcge500-octeon-mips64_octeon_v2_be (localhost)   10/11/13

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           1.13    0.00    0.27    0.08    0.00   98.52

Device:            tps    MB_read/s    MB_wrtn/s    MB_read    MB_wrtn
cfa               1.21         0.02         0.00         15          0
```

次に、**show system iostat detail** コマンドの出力例を示します。

```
(Cisco Controller) >show system iostat detail
Linux 2.6.21_mvlcge500-octeon-mips64_octeon_v2_be (localhost)   10/11/13

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.87    0.00    0.21    0.06    0.00   98.86

Device:         rrqm/s   wrqm/s     r/s     w/s    rMB/s    wMB/s avgrq-sz avgqu-sz
await  svctm  %util
cfa               8.42     0.15    0.84    0.09     0.01     0.00    28.79     0.02
23.41   7.20   0.67
```

show system top

システム上の CPU を最も駆使するタスクのリストを表示するには、**show system top** コマンドを使用します。

show system top

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが導入されました。

次に、**show system top** コマンドの出力例を示します。

```
(Cisco Controller) >show system top
top - 06:16:32 up 2 min,  0 users,  load average: 2.68, 1.05, 0.38
Tasks: 180 total,   1 running, 179 sleeping,   0 stopped,   0 zombie
Cpu0  :  0.0%us,  0.9%sy,  0.0%ni, 99.1%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu1  :  0.7%us,  0.3%sy,  0.0%ni, 98.7%id,  0.2%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu2  :  0.3%us,  0.2%sy,  0.0%ni, 97.9%id,  0.7%wa,  0.0%hi,  0.9%si,  0.0%st
Cpu3  :  8.6%us,  1.0%sy,  0.0%ni, 89.1%id,  0.8%wa,  0.0%hi,  0.6%si,  0.0%st
Cpu4  : 13.8%us,  6.9%sy,  0.0%ni, 77.0%id,  0.6%wa,  0.0%hi,  1.7%si,  0.0%st
Cpu5  : 32.9%us,  0.2%sy,  0.0%ni, 65.1%id,  0.7%wa,  0.0%hi,  1.1%si,  0.0%st
Cpu6  :  0.4%us,  0.2%sy,  0.0%ni, 98.5%id,  0.7%wa,  0.0%hi,  0.2%si,  0.0%st
Cpu7  : 15.6%us,  0.6%sy,  0.0%ni, 82.4%id,  0.7%wa,  0.0%hi,  0.7%si,  0.0%st
Cpu8  :  3.8%us,  0.4%sy,  0.0%ni, 95.2%id,  0.6%wa,  0.0%hi,  0.1%si,  0.0%st
Cpu9  :  0.7%us,  0.3%sy,  0.0%ni, 97.9%id,  0.2%wa,  0.0%hi,  0.8%si,  0.0%st
Mem:   1004116k total,   681232k used,   322884k free,      220k buffers
Swap:        0k total,        0k used,        0k free,   138696k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 1555 root      15   0  2556 1116  816 R    7  0.1   0:00.07 top
    1 root      18   0  4420  752  628 S    0  0.1   0:09.11 init
    2 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/0
    3 root      RT   0     0    0    0 S    0  0.0   0:00.00 posix_cpu_timer
    4 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-high/0
    5 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-timer/0
    6 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-tx/
    7 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-rx/
    8 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-block/0
    9 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-tasklet
   10 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-sched/0
   11 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-rcu/0
   12 root      RT   0     0    0    0 S    0  0.0   0:00.00 watchdog/0
   13 root      15 -10     0    0    0 S    0  0.0   0:00.00 desched/0
   14 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/1
   15 root      RT   0     0    0    0 S    0  0.0   0:00.00 posix_cpu_timer
   16 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-high/1
   17 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-timer/1
   18 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-tx/
   19 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-rx/
```

```
20 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-block/1
21 root     -51   0     0     0     0 S     0  0.0   0:00.02 softirq-tasklet
22 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-sched/1
23 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-rcu/1
24 root      RT   0     0     0     0 S     0  0.0   0:00.00 watchdog/1
25 root       5 -10     0     0     0 S     0  0.0   0:00.00 desched/1
26 root      RT   0     0     0     0 S     0  0.0   0:00.00 migration/2
27 root      RT   0     0     0     0 S     0  0.0   0:00.00 posix_cpu_timer
28 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-high/2
29 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-timer/2
30 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-tx/
31 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-rx/
32 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-block/2
33 root     -51   0     0     0     0 S     0  0.0   0:01.19 softirq-tasklet
34 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-sched/2
35 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-rcu/2
36 root      RT   0     0     0     0 S     0  0.0   0:00.00 watchdog/2
37 root       5 -10     0     0     0 S     0  0.0   0:00.00 desched/2
38 root      RT   0     0     0     0 S     0  0.0   0:00.00 migration/3
39 root      RT   0     0     0     0 S     0  0.0   0:00.00 posix_cpu_timer
40 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-high/3
41 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-timer/3
42 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-tx/
43 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-rx/
44 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-block/3
45 root     -51   0     0     0     0 S     0  0.0   0:00.72 softirq-tasklet
46 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-sched/3
47 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-rcu/3
48 root      RT   0     0     0     0 S     0  0.0   0:00.00 watchdog/3
49 root       5 -10     0     0     0 S     0  0.0   0:00.00 desched/3
50 root      RT   0     0     0     0 S     0  0.0   0:00.00 migration/4
51 root      RT   0     0     0     0 S     0  0.0   0:00.00 posix_cpu_timer
52 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-high/4
53 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-timer/4
54 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-tx/
55 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-rx/
56 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-block/4
57 root     -51   0     0     0     0 S     0  0.0   0:02.20 softirq-tasklet
58 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-sched/4
59 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-rcu/4
60 root      RT   0     0     0     0 S     0  0.0   0:00.00 watchdog/4
61 root       5 -10     0     0     0 S     0  0.0   0:00.00 desched/4
62 root      RT   0     0     0     0 S     0  0.0   0:00.00 migration/5
63 root      RT   0     0     0     0 S     0  0.0   0:00.00 posix_cpu_timer
64 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-high/5
65 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-timer/5
66 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-tx/
67 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-rx/
68 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-block/5
69 root     -51   0     0     0     0 S     0  0.0   0:01.43 softirq-tasklet
70 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-sched/5
71 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-rcu/5
72 root      RT   0     0     0     0 S     0  0.0   0:00.00 watchdog/5
73 root       5 -10     0     0     0 S     0  0.0   0:00.00 desched/5
74 root      RT   0     0     0     0 S     0  0.0   0:00.00 migration/6
75 root      RT   0     0     0     0 S     0  0.0   0:00.00 posix_cpu_timer
76 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-high/6
77 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-timer/6
78 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-tx/
79 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-net-rx/
80 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-block/6
81 root     -51   0     0     0     0 S     0  0.0   0:00.20 softirq-tasklet
82 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-sched/6
83 root     -51   0     0     0     0 S     0  0.0   0:00.00 softirq-rcu/6
```

```
 84 root      RT   0     0    0    0 S    0  0.0   0:00.00 watchdog/6
 85 root       5 -10     0    0    0 S    0  0.0   0:00.00 desched/6
 86 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/7
 87 root      RT   0     0    0    0 S    0  0.0   0:00.00 posix_cpu_timer
 88 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-high/7
 89 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-timer/7
 90 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-tx/
 91 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-rx/
 92 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-block/7
 93 root     -51   0     0    0    0 S    0  0.0   0:00.84 softirq-tasklet
 94 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-sched/7
 95 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-rcu/7
 96 root      RT   0     0    0    0 S    0  0.0   0:00.00 watchdog/7
 97 root       5 -10     0    0    0 S    0  0.0   0:00.00 desched/7
 98 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/8
 99 root      RT   0     0    0    0 S    0  0.0   0:00.00 posix_cpu_timer
100 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-high/8
101 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-timer/8
102 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-tx/
103 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-rx/
104 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-block/8
105 root     -51   0     0    0    0 S    0  0.0   0:00.07 softirq-tasklet
106 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-sched/8
107 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-rcu/8
108 root      RT   0     0    0    0 S    0  0.0   0:00.00 watchdog/8
109 root       5 -10     0    0    0 S    0  0.0   0:00.00 desched/8
110 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/9
111 root      RT   0     0    0    0 S    0  0.0   0:00.00 posix_cpu_timer
112 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-high/9
113 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-timer/9
114 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-tx/
115 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-net-rx/
116 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-block/9
117 root     -51   0     0    0    0 S    0  0.0   0:01.10 softirq-tasklet
118 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-sched/9
119 root     -51   0     0    0    0 S    0  0.0   0:00.00 softirq-rcu/9
120 root      RT   0     0    0    0 S    0  0.0   0:00.00 watchdog/9
121 root       5 -10     0    0    0 S    0  0.0   0:00.00 desched/9
122 root      -2 -20     0    0    0 S    0  0.0   0:01.14 events/0
123 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/1
124 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/2
125 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/3
126 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/4
127 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/5
128 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/6
129 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/7
130 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/8
131 root      -2 -20     0    0    0 S    0  0.0   0:00.00 events/9
132 root      15  -5     0    0    0 S    0  0.0   0:00.03 khelper
133 root      15  -5     0    0    0 S    0  0.0   0:00.00 kthread
165 root      20  -5     0    0    0 S    0  0.0   0:00.00 kblockd/0
166 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/1
167 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/2
168 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/3
169 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/4
170 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/5
171 root      15  -5     0    0    0 S    0  0.0   0:00.00 kblockd/6
172 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/7
173 root      20  -5     0    0    0 S    0  0.0   0:00.00 kblockd/8
174 root      10  -5     0    0    0 S    0  0.0   0:00.00 kblockd/9
212 root      21   0     0    0    0 S    0  0.0   0:00.00 pdflush
213 root      15   0     0    0    0 S    0  0.0   0:00.00 pdflush
214 root      16  -5     0    0    0 S    0  0.0   0:00.00 kswapd0
215 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/0
```

```
  216 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/1
  217 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/2
  218 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/3
  219 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/4
  220 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/5
  221 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/6
  222 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/7
  223 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/8
  224 root      10  -5     0    0    0 S    0  0.0   0:00.00 flush_filesd/9
  225 root      16  -5     0    0    0 S    0  0.0   0:00.00 aio/0
  226 root      16  -5     0    0    0 S    0  0.0   0:00.00 aio/1
  227 root      16  -5     0    0    0 S    0  0.0   0:00.00 aio/2
  228 root      16  -5     0    0    0 S    0  0.0   0:00.00 aio/3
  229 root      16  -5     0    0    0 S    0  0.0   0:00.00 aio/4
  230 root      16  -5     0    0    0 S    0  0.0   0:00.00 aio/5
  231 root      16  -5     0    0    0 S    0  0.0   0:00.00 aio/6
  232 root      20  -5     0    0    0 S    0  0.0   0:00.00 aio/7
  233 root      20  -5     0    0    0 S    0  0.0   0:00.00 aio/8
  234 root      20  -5     0    0    0 S    0  0.0   0:00.00 aio/9
  799 root      25   0     0    0    0 S    0  0.0   0:00.00 mtdblockd
  857 root      10  -5     0    0    0 S    0  0.0   0:00.04 kjournald
  868 root      10  -5     0    0    0 S    0  0.0   0:00.00 kjournald
  907 root      15   0     0    0    0 S    0  0.0   0:00.00 Octeon Poll Thr
  920 root      18   0  4420  804  628 D    0  0.1   0:00.00 insmod
  991 root      23   0     0    0    0 S    0  0.0   0:00.00 HATHREAD
 1014 root      15   0  4560  992  748 S    0  0.1   0:00.00 sshd
 1076 root      19   0  4484  880  748 S    0  0.1   0:00.00 gettyOrMwar
 1079 root      20   0  896m 480m  20m S    0 49.0   1:42.23 switchdrvr
 1238 root      16  -5     0    0    0 S    0  0.0   0:00.00 kjournald
 1245 root       0 -20     0    0    0 S    0  0.0   0:00.00 loop3
 1254 root      25   0 25880 3308 2556 S    0  0.3   0:00.62 licensed
 1554 root      16   0  4420  836  708 S    0  0.1   0:00.00 sh
```

show tacacs acct statistics

指定されたタグの詳細な無線周波数ID（RFID）情報を表示するには、**show tacacs acct statistics** コマンドを使用します。

show tacacs acct statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、詳細な RFID 情報を表示する例を示します。

```
(Cisco Controller) > show tacacs acct statistics
Accounting Servers:
Server Index..................................... 1
Server Address................................... 10.0.0.0
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 1
Retry Requests................................... 0
Accounting Response.............................. 0
Accounting Request Success....................... 0
Accounting Request Failure....................... 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. -1
Timeout Requests................................. 1
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

show tacacs athr statistics

TACACS+ サーバ許可の統計情報を表示するには、**show tacacs athr statistics** コマンドを使用します。

show tacacs athr statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、TACACS サーバ許可の統計情報を表示する例を示します。

```
(Cisco Controller) > show tacacs athr statistics
Authorization Servers:
Server Index..................................... 3
Server Address................................... 10.0.0.3
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 0
Retry Requests................................... 0
Received Responses............................... 0
Authorization Success............................ 0
Authorization Failure............................ 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

関連コマンド

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs auth statistics

show tacacs summary

show tacacs auth statistics

TACACS+ サーバ認証の統計情報を表示するには、**show tacacs auth statistics** コマンドを使用します。

show tacacs auth statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、TACACS サーバ認証の統計情報を表示する例を示します。

```
(Cisco Controller) > show tacacs auth statistics
Authentication Servers:
Server Index..................................... 2
Server Address................................... 10.0.0.2
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 0
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Error Responses.................................. 0
Restart Responses................................ 0
Follow Responses................................. 0
GetData Responses................................ 0
Encrypt no secret Responses...................... 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

show tacacs summary

TACACS+ サーバの要約情報を表示するには、**show tacacs summary** コマンドを使用します。

show tacacs summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、TACACS サーバの要約情報を表示する例を示します。

```
(Cisco Controller) > show tacacs summary
Authentication Servers
Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
2    10.0.0.1          49       Enabled   30
Accounting Servers
Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    10.0.0.0          49      Enabled    5
Authorization Servers
Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
3    10.0.0.3          49       Enabled   5
Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
4    2001:9:6:40::623  49       Enabled   5
...
```

関連コマンド

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs summary

show tacacs athr statistics

show tacacs auth statistics

show tech-support

Cisco Technical Assistance Center（TAC）から頻繁に要求される Cisco ワイヤレス LAN コントローラの変数を表示するには、**show tech-support** コマンドを使用します。

show tech-support

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次の例では、システム リソース情報を表示する方法を示します。

```
> show tech-support
Current CPU Load..............................  0%
System Buffers
   Max Free Buffers...........................  4608
   Free Buffers...............................  4604
   Buffers In Use.............................  4
Web Server Resources
   Descriptors Allocated......................  152
   Descriptors Used...........................  3
   Segments Allocated.........................  152
   Segments Used..............................  3
System Resources
   Uptime.....................................  747040 Secs
   Total Ram..................................  127552 Kbytes
   Free Ram...................................  19540 Kbytes
   Shared Ram.................................  0 Kbytes
   Buffer Ram.................................  460 Kbytes
```

show time

Cisco ワイヤレス LAN コントローラの日時を表示するには、**show time** コマンドを使用します。

show time

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、認証がイネーブルでないコントローラの日時を表示する例を示します。

```
> show time
Time..................................... Wed Apr 13 09:29:15 2011
Timezone delta........................... 0:0
Timezone location........................ (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
    NTP Polling Interval.....................     3600
     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              0           9.2.60.60       AUTH DISABLED
```

次に、NTP メッセージの認証に成功した結果、AUTH に成功する例を示します。

```
> show time
Time..................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
Timezone location........................ (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
    NTP Polling Interval.....................     3600
     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              1           9.2.60.60       AUTH SUCCESS
```

次に、受信パケットにエラーがある場合は、NTP メッセージ認証状態が AUTH の失敗を示す例を示します。

```
> show time
Time..................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
Timezone location........................ (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
    NTP Polling Interval.....................     3600
     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              10           9.2.60.60       AUTH FAILURE
```

次に、パケットの NTP サーバから応答がない場合、NTP メッセージ認証ステートが空白になる例を示します。

```
> show time
Time..................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
```

```
Timezone location.............................. (GMT +5:30) Colombo, New Delhi, Chennai,
 Kolkata
NTP Servers
    NTP Polling Interval.........................     3600
     Index     NTP Key Index     NTP Server      NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              11           9.2.60.60
```

関連コマンド

config time manual

config time ntp

config time timezone

config time timezone location

show trapflags

Cisco ワイヤレス LAN コントローラの Simple Network Management Protocol（SNMP）トラップ フラグを表示するには、**show trapflags** コマンドを使用します。

show trapflags

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし。

次に、コントローラの SNMP トラップ フラグを表示する例を示します。

```
> show trapflags
Authentication Flag.......................... Enable
Link Up/Down Flag............................ Enable
Multiple Users Flag.......................... Enable
Spanning Tree Flag........................... Enable
Client Related Traps
        802.11 Disassociation..................... Disable
        802.11 Association.........................Disabled
        802.11 Deauthenticate..................... Disable
        802.11 Authenticate Failure............... Disable
        802.11 Association Failure................ Disable
        Authentication.............................Disabled
        Excluded.................................. Disable
        Max Client Warning Threshold.............. 90%
       Nac-Alert Traps............................... Disabled
       RFID Related Traps
        Max RFIDs Warning Threshold..................... 90%

802.11 Security related traps
        WEP Decrypt Error......................... Enable
        IDS Signature Attack...................... Disable

Cisco AP
        Register.................................. Enable
        InterfaceUp............................... Enable
Auto-RF Profiles
        Load...................................... Enable
        Noise..................................... Enable
        Interference.............................. Enable
        Coverage.................................. Enable
Auto-RF Thresholds
        tx-power.................................. Enable
        channel................................... Enable
        antenna................................... Enable
AAA
        auth...................................... Enable
        servers................................... Enable
rogueap...................................... Enable
adjchannel-rogueap........................... Disabled
wps.......................................... Enable
configsave................................... Enable
IP Security
        esp-auth.................................. Enable
        esp-replay................................ Enable
        invalidSPI................................ Enable
```

```
        ike-neg..................................... Enable
        suite-neg................................... Enable
        invalid-cookie.............................. Enable
Mesh
        auth failure................................ Enabled
        child excluded parent....................... Enabled
        parent change............................... Enabled
        child moved................................. Enabled
        excessive parent change..................... Enabled
        onset SNR................................... Enabled
        abate SNR................................... Enabled
        console login............................... Enabled
        excessive association....................... Enabled
        default bridge group name................... Enabled
        excessive hop count......................... Disabled
        excessive children.......................... Enabled
        sec backhaul change......................... Disabled
```

関連コマンド

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

show traplog

Cisco ワイヤレス LAN コントローラの Simple Network Management Protocol（SNMP）トラップログを表示するには、**show traplog** コマンドを使用します。

show traplog

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**show traplog** コマンドの出力例を示します。

```
(Cisco Controller) > show traplog
Number of Traps Since Last Reset..... 2447
Number of Traps Since Log Last Displayed... 2447
Log System Time              Trap
--- ------------------------ ------------------------------------------------
  0 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:52:62:fe detected on Base Rad
                             io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
                             b/g) with RSSI: -78 and SNR: 10
  1 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:52:19:d8 detected on Base Rad
                             io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
                             b/g) with RSSI: -72 and SNR: 16
  2 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:26:a1:8d detected on Base Rad
                             io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
                             b/g) with RSSI: -82 and SNR: 6
  3 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:14:b3:4f detected on Base Rad
                             io MAC : 00:0b:85:18:b6:50  Interface no:1(802.11
                             b/g) with RSSI: -56 and SNR: 30
Would you like to display more entries? (y/n)
```

show tunnel profile-summary

すべてのプロファイルの要約を表示するには、**show tunnel profile** コマンドを使用します。

show tunnel profilesummary

構文の説明

summary	すべてのプロファイルの要約を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、すべてのプロファイルの要約を表示する例を示します。

```
show tunnel profile summary
```

show tunnel profile-detail

特定のプロファイルの詳細を表示するには、**show tunnel profile** コマンドを使用します。

show tunnel profiledetail *profile-name*

構文の説明

detail	特定のプロファイルの詳細を表示します。
profile-name	プロファイルの名前

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、特定のプロファイルに関する詳細を表示する例を示します。

```
show tunnel profile detail test
```

show tunnel eogre-summary

グローバル設定の要約を表示するには、**show tunnel eogre** コマンドを使用します。

show tunnel eogre summary

構文の説明	**summary** グローバル設定の要約を表示します。

コマンド デフォルト	なし

コマンド履歴	リリース	変更内容
	8.1	このコマンドが導入されました。

次に、グローバル設定の詳細を表示する例を示します。

```
(Cisco Controller) > show tunnel eogre summary
```

show tunnel eogre-statistics

EoGRE トンネル統計情報を表示するには、**show tunnel eogre** コマンドを使用します。

show tunnel eogrestatistics

構文の説明

statistics	EoGRE トンネル統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、EoGRE トンネル統計情報の詳細を表示する例を示します。

```
show tunnel eogre statistics
```

show tunnel eogre-domain-summary

EoGRE ドメイン サマリーを表示するには、**show tunnel eogre** コマンドを使用します。

show tunnel eogredomainsummary

構文の説明

summary	EoGRE ドメイン サマリーを表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、EoGRE ドメイン サマリーを表示する例を示します。

```
show tunnel eogre domain summary
```

show tunnel eogre gateway

EoGRE トンネル ゲートウェイの要約および統計情報を表示するには、**show tunnel eogre** コマンドを使用します。

show tunnel eogre gateway {**summary** | **statistics**}

構文の説明

summary	EoGRE トンネル ゲートウェイの要約を表示します。
statistics	EoGRE トンネル ゲートウェイの統計情報を表示します。

コマンド デフォルト

なし

使用上のガイドライン

show tunnel eogre gateway summaryコマンドは、FlexConnect 中央スイッチング クライアントおよびローカル モード AP クライアントの詳細のみを一覧表示します。FlexConnect ローカル スイッチング クライアントの詳細を表示するには、 **show ap eogre gateway** *ap-name* コマンドを使用します。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。
8.5	**statistics** パラメータが追加されました。

show watchlist

クライアントの監視リストを表示するには、**show watchlist** コマンドを使用します。

show watchlist

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

次に、クライアントの監視リストの情報を表示する例を示します。

```
(Cisco Controller) >show watchlist
client watchlist state is disabled
```

show wlan

特定の無線 LAN または外部アクセス ポイントの設定情報、または無線 LAN の要約情報を表示するには、**show wlan** コマンドを使用します。

show wlan { **apgroups** | **summary** | *wlan_id* | **foreignAp** | **lobby-admin-access** }

構文の説明

apgroups	アクセス ポイント グループ情報を表示します。
summary	すべての無線 LAN の要約を表示します。
wlan_id	WLAN の設定を表示します。無線 LAN ID の範囲は 1 ～ 512 です。
foreignAp	外部アクセス ポイントのサポート設定を表示します。

コマンド デフォルト

なし

使用上のガイドライン

PMK キャッシュを作成する 802.1x クライアント セキュリティ タイプでは、セッション タイムアウトが無効になっている場合、設定できる最大セッション タイムアウトは 86400 秒です。PMK キャッシュが作成されない、オープン、WebAuth、PSK などのその他のクライアント セキュリティでは、セッション タイムアウトが無効になっている場合、セッション タイムアウト値は [infinite] と表示されます。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、wlan_id 1 の無線 LAN のサマリーを表示する例を示します。

```
(Cisco Controller) >show wlan 1
WLAN Identifier.................................. 1
Profile Name..................................... aicha
Network Name (SSID).............................. aicha
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control
   RADIUS Profiling Status ...................... Disabled
   DHCP ......................................... Disabled
   HTTP ......................................... Disabled
Client Profiling Status ..................... Disabled
   DHCP ......................................... Disabled
   HTTP ......................................... Disabled
   Radius-NAC State.............................. Enabled
   SNMP-NAC State................................ Enabled
Quarantine VLAN.................................. 0
```

```
Maximum number of Associated Clients.............. 0
Maximum number of Clients per AP Radio........... 200
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
User Idle Timeout................................ 300 seconds
User Idle Threshold.............................. 0 Bytes
NAS-identifier................................... Talwar1
CHD per WLAN..................................... Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ management
Multicast Interface.............................. Not Configured
WLAN IPv4 ACL.................................... unconfigured
WLAN IPv6 ACL.................................... unconfigured
mDNS Status...................................... Disabled
mDNS Profile Name................................ unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Static IP client tunneling....................... Enabled
PMIPv6 Mobility Type............................. none
Quality of Service............................... Silver (best effort)
Per-SSID Rate Limits............................. Upstream      Downstream
Average Data Rate................................   0             0
Average Realtime Data Rate.......................   0             0
Burst Data Rate..................................   0             0
Burst Realtime Data Rate.........................   0             0
Per-Client Rate Limits........................... Upstream      Downstream
Average Data Rate................................   0             0
Average Realtime Data Rate.......................   0             0
Burst Data Rate..................................   0             0
Burst Realtime Data Rate.........................   0             0
Scan Defer Priority.............................. 4,5,6
Scan Defer Time.................................. 100 milliseconds
WMM.............................................. Allowed
WMM UAPSD Compliant Client Support............... Disabled
Media Stream Multicast-direct.................... Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
Passive Client Feature........................... Disabled
IPv6 Support..................................... Disabled
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
DTIM period for 802.11a radio.................... 1
DTIM period for 802.11b radio.................... 1
Radius Servers
   Authentication................................ Global Servers
   Accounting.................................... Global Servers
   Interim Update.............................. Disabled
   Dynamic Interface............................. Disabled
Local EAP Authentication......................... Enabled (Profile 'Controller_Local_EAP')
Radius NAI-Realm................................. Enabled
Security
   802.11 Authentication:........................ Open System
    FT Support.................................... Disabled
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
      WPA2 (RSN IE)............................... Enabled
```

```
        TKIP Cipher..................................... Disabled
        AES Cipher...................................... Enabled
Auth Key Management
        802.1x.......................................... Enabled
        PSK............................................. Disabled
        CCKM............................................ Enabled
        FT(802.11r)..................................... Disabled
        FT-PSK(802.11r)................................. Disabled
        PMF-1X(802.11w)................................. Enabled
        PMF-PSK(802.11w)................................ Disabled
FT Reassociation Timeout................................ 20
FT Over-The-Air mode.................................... Enabled
FT Over-The-Ds mode..................................... Enabled
      GTK Randomization................................. Disabled
      SKC Cache Support................................. Disabled
      CCKM TSF Tolerance................................ 1000
   Wi-Fi Direct policy configured.......................... Disabled
   EAP-Passthrough......................................... Disabled
CKIP ..................................... Disabled
   IP Security............................................. Disabled
   IP Security Passthru.................................... Disabled
   Web Based Authentication................................ Disabled
   Web-Passthrough......................................... Disabled
   Conditional Web Redirect................................ Disabled
   Splash-Page Web Redirect................................ Disabled
   Auto Anchor............................................. Disabled
   FlexConnect Local Switching............................. Enabled
   flexconnect Central Dhcp Flag........................... Disabled
   flexconnect nat-pat Flag................................ Disabled
   flexconnect Dns Override Flag........................... Disabled
   FlexConnect Vlan based Central Switching ..... Disabled
   FlexConnect Local Authentication........................ Disabled
   FlexConnect Learn IP Address............................ Enabled
   Client MFP.............................................. Optional
   PMF..................................... Disabled
   PMF Association Comeback Time........................... 1
   PMF SA Query RetryTimeout............................... 200
   Tkip MIC Countermeasure Hold-down Timer....... 60
Call Snooping........................................... Disabled
Roamed Call Re-Anchor Policy............................ Disabled
SIP CAC Fail Send-486-Busy Policy....................... Enabled
SIP CAC Fail Send Dis-Association Policy......... Disabled
KTS based CAC Policy.................................... Disabled
Band Select............................................. Disabled
Load Balancing.......................................... Disabled
 Mobility Anchor List
 WLAN ID     IP Address            Status
 -------     ---------------       ------
802.11u..................................... Enabled
  Network Access type..................... Chargeable Public Network
  Internet service........................ Enabled
  Network Authentication type............. Not Applicable
  HESSID.................................. 00:00:00:00:00:00
  IP Address Type Configuration
    IPv4 Address type.....................  Available
    IPv6 Address type.....................  Not Known

  Roaming Consortium List
    Index       OUI List     In Beacon
    -----   --------------   ---------
      1         313131       Yes
      2         DDBBCC       No
      3         DDDDDD       Yes
 Realm configuration summary
```

```
    Realm index..................................... 1
    Realm name...................................... jobin
      EAP index..................................... 1
      EAP method.................................... Unsupported
    Index   Inner Authentication           Authentication Method
    -----   --------------------           ---------------------
        1                Credential Type                    SIM
        2   Tunneled Eap Credential Type                    SIM
        3                Credential Type                    SIM
        4                Credential Type                   USIM
        5                Credential Type         Hardware Token
        6                Credential Type              SoftToken
  Domain name configuration summary
    Index  Domain name
    -------------------
        1   rom3
        2   ram
        3   rom1

Hotspot 2.0..................................... Enabled

  Operator name configuration summary
    Index   Language   Operator name
    -----   --------   -------------
        1         ros   Robin

  Port config summary
 Index   IP protocol   Port number   Status
    -----   -----------   -----------   -------
        1             1             0    Closed
        2             1             0    Closed
        3             1             0    Closed
        4             1             0    Closed
        5             1             0    Closed
        6             1             0    Closed
        7             1             0    Closed
 WAN Metrics Info
    Link status.................................. Up
    Symmetric Link............................... No
    Downlink speed............................... 4 kbps
    Uplink speed................................. 4 kbps

MSAP Services................................... Disabled
Local Policy
----------------
Priority  Policy Name
--------  ---------------
   1        Teacher_access_policy
```

次に、すべての WLAN のサマリーを表示する例を示します。

```
(Cisco Controller) >show wlan summary
Number of WLANs................................. 1

WLAN ID  WLAN Profile Name / SSID               Status    Interface Name        PMIPv6
Mobility
-------  -------------------------------------  --------  --------------------
---------------
1        apsso / apsso                          Disabled  management            none
```

次に、外部アクセス ポイントのサポート設定を表示する例を示します。

```
(Cisco Controller) >show wlan foreignap
Foreign AP support is not enabled.
```

次に、AP グループを表示する例を示します。

```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups..................... 1
Site Name..................................... APuser
Site Description.............................. <none>
Venue Name.................................... Not configured
Venue Group Code.............................Unspecified
Venue Type Code..............................Unspecified
Language Code................................. Not configured
AP Operating Class............................ 83,84,112,113,115,116,117,118,123
RF Profile
----------
2.4 GHz band.................................. <none>
5 GHz band.................................... <none>
WLAN ID          Interface          Network Admission Control          Radio Policy
-------          -----------        -------------------------          ------------
 14              int_4                Disabled                          All
AP Name             Slots  AP Model             Ethernet MAC       Location
Port  Country  Priority
------------------  -----  -------------------  -----------------  ----------------
----  -------  --------
Ibiza                2     AIR-CAP2602I-A-K9    44:2b:03:9a:8a:73  default location  1
    US       1
Larch                2     AIR-CAP3502E-A-K9    f8:66:f2:ab:23:95  default location  1
    US       1

Zest                 2     AIR-CAP3502I-A-K9    00:22:90:91:6d:b6               ren  1
    US       1

Number of Clients............................. 1

MAC Address       AP Name          Status        Device Type
----------------- ------------- ------------- -----------------

24:77:03:89:9b:f8      ap2       Associated      Android
```

show wps ap-authentication summary

コントローラのアクセス ポイント ネイバー認証の設定を表示するには、**show wps ap-authentication summary** コマンドを使用します。

show wps ap-authentication summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Wireless Protection System（WPS）アクセス ポイント ネイバー認証のサマリーを表示する例を示します。

```
(Cisco Controller) > show wps ap-authentication summary
AP neighbor authentication is <disabled>.
Authentication alarm threshold is 1.
RF-Network Name: <B1>
```

関連コマンド

config wps ap-authentication

show wps cids-sensor

侵入検知システム（IDS）センサーの要約情報、または指定した Wireless Protection System（WPS）IDS センサーの詳細情報を表示するには、**show wps cids-sensor** コマンドを使用します。

show wps cids-sensor {**summary** | **detail** *index*}

構文の説明

summary	センサー設定のサマリーを表示します。
detail	選択したセンサーのすべての設定を表示します。
index	IDS センサー ID。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、選択したセンサーのすべての設定を表示する例を示します。

```
(Cisco Controller) > show wps cids-sensor detail1
IP Address..................................... 10.0.0.51
Port........................................... 443
Query Interval................................. 60
Username....................................... Sensor_user1
Cert Fingerprint............................... SHA1:
00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Query State.................................... Disabled
Last Query Result.............................. Unknown
Number of Queries Sent......................... 0
```

関連コマンド

config wps ap-authentication

show wps mfp

管理フレーム保護（MFP）情報を表示するには、**show wps mfp** コマンドを使用します。

show wps mfp {**summary** | **statistics**}

構文の説明

summary	MFP の設定およびステータスを表示します。
statistics	MFP の統計情報を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、MFP の設定およびステータスのサマリーを表示する例を示します。

```
(Cisco Controller) > show wps mfp summary
Global Infrastructure MFP state.................. DISABLED (*all infrastructure
settings are overridden)
Controller Time Source Valid..................... False
                                  WLAN       Infra.      Client
WLAN ID  WLAN Name                Status     Protection  Protection
-------  -------------------------  ---------  ----------  ----------
1        homeap                   Disabled   *Enabled    Optional but inactive
 (WPA2 not configured)
2        7921                     Enabled    *Enabled    Optional but inactive
 (WPA2 not configured)
3        open1                    Enabled    *Enabled    Optional but inactive
 (WPA2 not configured)
4        7920                     Enabled    *Enabled    Optional but inactive
 (WPA2 not configured)
                     Infra.             Operational     --Infra. Capability--
AP Name              Validation  Radio  State           Protection  Validation
-------------------  ----------  -----  --------------  ----------  ----------
AP1252AG-EW          *Enabled    b/g    Down            Full        Full
                                 a      Down            Full        Full
```

次に、MFP 統計情報の表示方法の例を示します。

```
(Cisco Controller) > show wps mfp statistics
BSSID             Radio Validator AP         Last Source Addr  Found  Error Type
     Count      Frame Types
----------------- ----- -------------------- ----------------- ------ ----------
---- ---------- -----------
no errors
```

関連コマンド

config wps mfp

show wps shun-list

侵入検知システム（IDS）センサーの回避リストを表示するには、**show wps shun-list** コマンドを使用します。

show wps shun-list

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、IDS システム センサーの回避リストを表示する例を示します。

```
(Cisco Controller) > show wps shun-list
```

関連コマンド

config wps shun-list re-sync

show wps signature detail

インストールされているシグニチャを表示するには、**show wps signature detail** コマンドを使用します。

show wps signature detail *sig-id*

構文の説明

sig-id	インストールされているシグニチャのシグニチャ ID。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、標準シグニチャ 1 によって検出される攻撃の詳細を表示する例を示します。

```
(Cisco Controller) > show wps signature detail 1
Signature-ID..................................... 1
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. standard
FrameType........................................ management
State............................................ enabled
Action........................................... report
Tracking......................................... per Signature and Mac
Signature Frequency.............................. 500 pkts/interval
Signature Mac Frequency.......................... 300 pkts/interval
Interval......................................... 10 sec
Quiet Time....................................... 300 sec
Description...................................... Broadcast Deauthentication Frame
Patterns:
                0(Header):0x0:0x0
                4(Header):0x0:0x0
```

関連コマンド

config wps signature

config wps signature frequency

config wps signature mac-frequency

config wps signature interval

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

show wps signature events

特定の標準シグニチャまたはカスタムシグニチャによって検出された攻撃の詳細情報を表示するには、**show wps signature events** コマンドを使用します。

show wps signature events {**summary** | {**standard** | **custom**} *precedenceID* {**summary** | **detailed**}

構文の説明

summary	すべてのシグニチャ トラッキングの要約情報を表示します。
standard	標準侵入検知システム（IDS）シグニチャの設定を表示します。
custom	カスタムIDSシグニチャの設定を表示します。
precedenceID	シグニチャ優先 ID の値。
detailed	送信元 MAC アドレス トラッキングの詳細を表示します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース7.6以前のリリースで導入されました。

次に、すべての有効なシグニチャによって検出された攻撃の数を表示する例を示します。

```
(Cisco Controller) > show wps signature events summary
Precedence  Signature Name       Type      # Events
----------  -------------------- --------  --------
1           Bcast deauth         Standard      2
2           NULL probe resp 1    Standard      1
```

次に、標準シグニチャ1によって検出された攻撃の要約情報を表示する例を示します。

```
(Cisco Controller) > show wps signature events standard 1 summary
Precedence..................................... 1
Signature Name................................. Bcast deauth
Type........................................... Standard
Number of active events........................ 2
Source MAC Addr    Track Method   Frequency # APs Last Heard
-----------------  -------------- --------- -----
-----------------------
```

```
00:a0:f8:58:60:dd  Per Signature  50        1     Wed Oct 25 15:03:05
2006
00:a0:f8:58:60:dd  Per Mac        30        1     Wed Oct 25 15:02:53
2006
```

関連コマンド

config wps signature frequency

config wps signature mac-frequency

config wps signature interval

config wps signature quiet-time

config wps signature reset

config wps signature

show wps signature summary

show wps summary

show wps signature summary

コントローラにインストールされているすべての標準シグニチャとカスタム シグニチャの要約を個々に表示するには、**show wps signature summary** コマンドを使用します。

show wps signature summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、標準シグニチャおよびカスタム シグニチャのすべてのサマリーを表示する例を示します。

```
(Cisco Controller) > show wps signature summary
Signature-ID..................................... 1
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. standard
FrameType........................................ management
State............................................ enabled
Action........................................... report
Tracking..................................... per Signature and Mac
Signature Frequency.............................. 50 pkts/interval
Signature Mac Frequency.......................... 30 pkts/interval
Interval......................................... 1 sec
Quiet Time....................................... 300 sec
Description...................................... Broadcast
Deauthentication Frame
Patterns:
                0(Header):0x00c0:0x00ff
                4(Header):0x01:0x01
...
```

関連コマンド

config wps signature frequency

config wps signature interval

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps summary

config wps signature mac-frequency

config wps signature

show wps summary

Wireless Protection System（WPS）の要約情報を表示するには、**show wps summary** コマンドを使用します。

show wps summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、WPS の要約情報を表示する例を示します。

```
(Cisco Controller) > show wps summary
Auto-Immune
  Auto-Immune..................................... Disabled
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
Trusted AP Policy
  Management Frame Protection.................... Disabled
  Mis-configured AP Action....................... Alarm Only
    Enforced encryption policy................... none
    Enforced preamble policy..................... none
    Enforced radio type policy................... none
    Validate SSID................................ Disabled
  Alert if Trusted AP is missing................. Disabled
  Trusted AP timeout............................. 120
Untrusted AP Policy
  Rogue Location Discovery Protocol.............. Disabled
    RLDP Action.................................. Alarm Only
  Rogue APs
    Rogues AP advertising my SSID................ Alarm Only
    Detect and report Ad-Hoc Networks............ Enabled
  Rogue Clients
    Validate rogue clients against AAA........... Enabled
    Detect trusted clients on rogue APs.......... Alarm Only
  Rogue AP timeout............................... 1300
Signature Policy
```

```
  Signature Processing.......................... Enabled
...
```

関連コマンド

config wps signature frequency

config wps signature interval

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature mac-frequency

show wps summary

config wps signature

config wps signature interval

show wps wips statistics

コントローラ上の Cisco Wireless Intrusion Prevention System（wIPS）の現在の動作状態を表示するには、**show wps wips statistics** コマンドを使用します。

show wps wips statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、wIPS 動作の統計情報を表示する例を示します。

```
(Cisco Controller) > show wps wips statistics
Policy Assignment Requests..... 1
Policy Assignment Responses..... 1
Policy Update Requests..... 0
Policy Update Responses..... 0
Policy Delete Requests..... 0
Policy Delete Responses..... 0
Alarm Updates..... 13572
Device Updates..... 8376
Device Update Requests..... 0
Device Update Responses..... 0
Forensic Updates..... 1001
Invalid WIPS Payloads..... 0
Invalid Messages Received..... 0
NMSP Transmitted Packets..... 22950
NMSP Transmit Packets Dropped..... 0
NMSP Largest Packet..... 1377
```

関連コマンド

config 802.11 enable

config ap mode

config ap monitor-mode

show ap config

show ap monitor-mode summary

show wps wips summary

show wps wips summary

Wireless Control System（WCS）がコントローラに転送する適応型 Cisco Wireless Intrusion Prevention System（wIPS）を表示するには、**show wps wips summary** コマンドを使用します。

show wps wips summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、wIPS の設定のサマリーを表示する例を示します。

```
(Cisco Controller) > show wps wips summary
Policy Name..................................... Default
Policy Version.................................. 3
```

関連コマンド

config 802.11 enable

config ap mode

config ap monitor-mode

show ap config

show ap monitor-mode summary

show wps wips statistics

show wps ap-authentication summary

コントローラのアクセス ポイント ネイバー認証の設定を表示するには、**show wps ap-authentication summary** コマンドを使用します。

show wps ap-authentication summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Wireless Protection System（WPS）アクセス ポイント ネイバー認証のサマリーを表示する例を示します。

```
(Cisco Controller) > show wps ap-authentication summary
AP neighbor authentication is <disabled>.
Authentication alarm threshold is 1.
RF-Network Name: <B1>
```

関連コマンド

config wps ap-authentication

第 VIII 部

その他のコマンド

- その他のコマンド：1 （1851 ページ）
- その他のコマンド：1 （1857 ページ）

その他のコマンド：1

- cping （1852 ページ）
- eping （1853 ページ）
- mping （1854 ページ）
- ping （1855 ページ）

cping

CAPWAP を使用してモビリティ データ トラフィックをテストするには、**cping** コマンドを使用します。

cping *mobility_peer_IP_address*

構文の説明

mobility_peer_IP_address	ピア モビリティ コントローラの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.5	このコマンドは、コントローラのリリース 7.5 で導入されました。

使用上のガイドライン

このコマンドは、新しいモビリティ アーキテクチャを使用してモビリティ データ トラフィックをテストします。

次に、ピア モビリティ IP アドレスが 172.12.35.31 のコントローラのデータ トラフィックをテストする例を示します。

```
(Cisco Controller) >cping 172.12.35.31
```

eping

2 台の Cisco WLC 間のモビリティ Ethernet over IP（EoIP）データ パケット通信をテストするには、**eping** コマンドを使用します。

eping *mobility_peer_IP_address*

構文の説明

mobility_peer_IP_address	モビリティ グループに属するコントローラの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

使用上のガイドライン

このコマンドは、管理インターフェイス上のモビリティ データ トラフィックをテストします。

（注） この PING テストは、インターネット制御メッセージ プロトコル（ICMP）ベースではありません。「ping」という用語は、エコー要求とエコー応答メッセージを示すために使用されます。

このコマンドでは IPv6 アドレス形式はサポートされません。

次に、EoIP データ パケットをテストし、モビリティ グループに属するコントローラの IP アドレスを 172.12.35.31 に設定する例を示します。

```
(Cisco Controller) >eping 172.12.35.31
```

mping

2 台の Cisco WLC 間のモビリティ UDP 制御パケット通信をテストするには、**mping** コマンドを使用します。

mping *mobility_peer_IP_address*

構文の説明

mobility_peer_IP_address	モビリティ グループに属するコントローラの IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン

このテストは、モビリティ UDP ポート 16666 で実行します。このテストでは、管理インターフェイスを介してモビリティ制御パケットが到達できるかどうかを確認します。

（注） この PING テストは、インターネット制御メッセージ プロトコル（ICMP）ベースではありません。「ping」という用語は、エコー要求とエコー応答メッセージを示すために使用されます。

次に、モビリティ UDP 制御パケット通信をテストし、モビリティ グループに属する Cisco WLC の IP アドレスを 172.12.35.31 に設定する例を示します。

```
(Cisco Controller) >mping 172.12.35.31
```

ping

指定された IP アドレスに ICMP エコー パケットを送信します。

ping *ip-addr interface-name*

構文の説明

ip-addr	ICMP エコー パケットを送信しようとしているインターフェイスの IP アドレス。
interface-name	ICMP エコー パケットを送信しようとしているインターフェイスの名前。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

ping コマンドを実行すると、「osapi_ping_rx process」で CPU 使用率が最大 98 % に急上昇します。**ping** コマンドの実行中は、Cisco WLC 上の端末および Web アクティビティがブロックされます。

例

次に、インターフェイスに ICMP エコー パケットを送信する例を示します。

```
(Cisco Controller) >ping 209.165.200.225 dyn-interface-1
```

その他のコマンド：1

- capwap ap controller ip address （1859 ページ）
- capwap ap dot1x （1860 ページ）
- capwap ap hostname （1861 ページ）
- capwap ap ip address （1862 ページ）
- capwap ap ip default-gateway （1863 ページ）
- capwap ap log-server （1864 ページ）
- capwap ap mode （1865 ページ）
- capwap ap primary-base （1866 ページ）
- capwap ap primed-timer （1867 ページ）
- capwap ap secondary-base （1868 ページ）
- capwap ap tertiary-base （1869 ページ）
- lwapp ap controller ip address （1870 ページ）
- reset system at （1871 ページ）
- reset system in （1872 ページ）
- reset system cancel （1873 ページ）
- reset system notify-time （1874 ページ）
- reset peer-system （1875 ページ）
- save config （1876 ページ）
- transfer download certpasswor （1877 ページ）
- transfer download datatype （1878 ページ）
- transfer download datatype icon （1880 ページ）
- transfer download filename （1881 ページ）
- transfer download mode （1882 ページ）
- transfer download password （1883 ページ）
- transfer download path （1884 ページ）
- transfer download port （1885 ページ）
- transfer download serverip （1886 ページ）
- transfer download start （1887 ページ）
- transfer download tftpPktTimeout （1888 ページ）

- transfer download tftpMaxRetries （1889 ページ）
- transfer download username （1890 ページ）
- transfer encrypt （1891 ページ）
- transfer upload datatype （1892 ページ）
- transfer upload filename （1894 ページ）
- transfer upload mode （1895 ページ）
- transfer upload pac （1896 ページ）
- transfer upload password （1897 ページ）
- transfer upload path （1898 ページ）
- transfer upload peer-start （1899 ページ）
- transfer upload port （1900 ページ）
- transfer upload serverip （1901 ページ）
- transfer upload start （1902 ページ）
- transfer upload username （1903 ページ）

capwap ap controller ip address

アクセス ポイントのコンソール ポートから CAPWAP アクセス ポイントにコントローラの IP アドレスを設定するには、**capwap ap controller ip address** コマンドを使用します。

capwap ap controller ip address *A.B.C.D*

構文の説明

A.B.C.D	コントローラの IP アドレス。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。このコマンドは、IPv4 アドレスのみに適用されます。

（注） アクセス ポイントで Cisco IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、CAPWAP アクセス ポイントにコントローラ IP アドレス 10.23.90.81 を設定する例を示します。

```
ap_console >capwap ap controller ip address 10.23.90.81
```

capwap ap dot1x

アクセス ポイントのコンソール ポートから CAPWAP アクセス ポイントに dot1x ユーザ名とパスワードを設定するには、**capwap ap dot1x** コマンドを使用します。

capwap ap dot1x username *user_name* **password** *password*

構文の説明

user_name	Dot1x ユーザ名。
password	Dot1x パスワード。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。

（注） アクセス ポイントで Cisco Access Point IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、dot1x のユーザ名 ABC とパスワード pass01 を設定する例を示します。

```
ap_console >capwap ap dot1x username ABC password pass01
```

capwap ap hostname

アクセス ポイントのコンソール ポートからアクセス ポイントのホスト名を設定するには、**capwap ap hostname** コマンドを使用します。

capwap ap hostname *host_name*

構文の説明

host_name	アクセス ポイントのホスト名。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。

（注） アクセス ポイントで Cisco IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。このコマンドは、private-config なしで Cisco Lightweight AP IOS ソフトウェア リカバリ イメージ（rcvk9w8）でのみ使用できます。**clear capwap private-config** コマンドを使用して、private-config を削除できます。

次に、capwap アクセス ポイントにホスト名 WLC を設定する例を示します。

```
ap_console >capwap ap hostname WLC
```

capwap ap ip address

アクセス ポイントのコンソール ポートから CAPWAP アクセス ポイントに IP アドレスを設定するには、**capwap ap ip address** コマンドを使用します。

capwap ap ip address *A.B.C.D*

構文の説明

A.B.C.D	IP アドレス

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。 このコマンドは、IPv4 アドレス形式のみをサポートします。

（注） アクセス ポイントで Cisco Access Point IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、CAPWAP アクセス ポイントに IP アドレス 10.0.0.1 を設定する例を示します。

```
ap_console >capwap ap ip address 10.0.0.1
```

capwap ap ip default-gateway

アクセス ポイントのコンソール ポートからデフォルト ゲートウェイを設定するには、**capwap ap ip default-gateway** コマンドを使用します。

capwap ap ip default-gateway *A.B.C.D*

構文の説明

A.B.C.D	capwap アクセス ポイントのデフォルト ゲートウェイ アドレス。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。 このコマンドは、IPv4 アドレス形式のみをサポートします。

（注） アクセス ポイントで Cisco Access Point IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、デフォルト ゲートウェイ アドレスが 10.0.0.1 の CAPWAP アクセス ポイントを設定する例を示します。

```
ap_console >capwap ap ip default-gateway 10.0.0.1
```

capwap ap log-server

システム ログ サーバをすべての CAPWAP エラーを記録するように設定するには、**capwap ap log-server** コマンドを使用します。

capwap ap log-server *A.B.C.D*

構文の説明

A.B.C.D	Syslog サーバの IP アドレス。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。 このコマンドは、IPv4 アドレス形式のみをサポートします。

（注） アクセス ポイントで Cisco Access Point IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、IP アドレス 10.0.0.1 の Syslog サーバを設定する例を示します。

```
ap_console >capwap ap log-server 10.0.0.1
```

capwap ap mode

アクセス ポイントでローカルまたはブリッジ モードを設定するには、**capwap ap mode** コマンドを使用します。

capwap ap mode local | **bridge**

構文の説明

local	アクセス ポイントをローカル モードで設定します。
bridge	アクセス ポイントをブリッジ モードで設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
8.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。

（注） このコマンドを実行すると、アクセス ポイントが再起動します。

次に、アクセス ポイントでブリッジ モードを設定する例を示します。

```
ap_console #capwap ap mode bridge
```

capwap ap primary-base

アクセス ポイントのコンソール ポートから CAPWAP アクセス ポイントにプライマリ コントローラの名前と IP アドレスを設定するには、**capwap ap primary-base** コマンドを使用します。

（注） このコマンドは、Cisco Wave 2 AP の IPv4 および IPv6 アドレスを設定します。

capwap ap primary-base *WORD A.B.C.D*

構文の説明

WORD	プライマリ コントローラの名前。
A.B.C.D	プライマリ コントローラの IP アドレス。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートからイネーブル モード（昇格されたアクセス）で入力する必要があります。

次に、CAPWAP アクセス ポイントに、プライマリ コントローラ名 WLC1 とプライマリ コントローラの IP アドレス 209.165.200.225 を設定する例を示します。

```
ap_console >capwap ap primary-base WLC1 209.165.200.225
```

capwap ap primed-timer

用意されたタイマーを CAPWAP アクセス ポイントに設定するには、**capwap ap primed-timer** コマンドを使用します。

capwap ap primed-timer {**enable** | **disable**}

構文の説明

enable	用意されたタイマーの設定をイネーブルにします
disable	用意されたタイマーの設定をディセーブルにします。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。

（注） アクセス ポイントで Cisco Access Point IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、用意されたタイマーの設定をイネーブルにする例を示します。

```
ap_console >capwap ap primed-timer enable
```

capwap ap secondary-base

アクセス ポイントのコンソール ポートから CAPWAP アクセス ポイントにセカンダリ Cisco WLC の名前と IP アドレスを設定するには、**capwap ap secondary-base** コマンドを使用します。

capwap ap secondary-base *controller_name controller_ip_address*

構文の説明

controller_name	セカンダリ Cisco WLC の名前。
controller_ip_address	セカンダリ Cisco WLC の IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。 このコマンドは、IPv4 アドレス形式のみをサポートします。

（注） アクセス ポイントで Cisco Access Point IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、セカンダリ Cisco WLC の名前 WLC2 およびセカンダリ Cisco WLC の IP アドレス 209.165.200.226 を CAPWAP アクセス ポイントに設定する例を示します。

```
ap_console >capwap ap secondary-base WLC2 209.165.200.226
```

capwap ap tertiary-base

アクセス ポイントのコンソール ポートから CAPWAP アクセス ポイントにターシャリ Cisco WLC の名前と IP アドレスを設定するには、**capwap ap tertiary-base** コマンドを使用します。

capwap ap tertiary-base *WORDA.B.C.D*

構文の説明

WORD	ターシャリ Cisco WLC の名前。
A.B.C.D	ターシャリ Cisco WLC の IP アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 アドレス形式のみをサポートします。

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。 このコマンドは、IPv4 アドレス形式のみをサポートします。

（注） アクセス ポイントで Cisco IOS Release 12.3(11)JX1 以降のリリースが実行されている必要があります。

次に、WLC3 という名前のターシャリ Cisco WLC およびセカンダリ Cisco WLC の IP アドレス 209.165.200.227 を CAPWAP アクセス ポイントに設定する例を示します。

```
ap_console >capwap ap tertiary-base WLC3 209.165.200.227
```

lwapp ap controller ip address

アクセス ポイントのコンソール ポートから FlexConnect アクセス ポイントに Cisco WLC の IP アドレスを設定するには、**lwapp ap controller ip address** コマンドを使用します。

lwapp ap controller ip address *A.B.C.D*

構文の説明

A.B.C.D	コントローラの IP アドレス。

コマンド デフォルト

なし

使用上のガイドライン

このコマンドはアクセス ポイントのコンソール ポートから入力する必要があります。このコマンドは、IPv4 アドレスのみに適用されます。

アクセス ポイントのコンソール ポートを使用してアクセス ポイントの FlexConnect 設定を変更する前に、アクセス ポイントをスタンドアロン モード（コントローラに接続されていない状態）にし、**clear lwapp private-config** コマンドを使用して現在の LWAPP プライベート設定を削除する必要があります。

（注） アクセス ポイントで Cisco IOS Release 12.3(11)JX1 以上のリリースが実行されている必要があります。

次に、FlexConnect アクセス ポイントにコントローラ IP アドレス 10.92.109.1 を設定する例を示します。

```
ap_console > lwapp ap controller ip address 10.92.109.1
```

reset system at

指定した時間にシステムをリセットするには、**reset system at** コマンドを使用します。

reset system at YYYY-MM-DD HH : MM : SS image {**no-swap** | **swap**} **reset-aps** [**save-config**]

構文の説明

YYYY-MM-DD	日付を指定します。
HH: MM: SS	24 時間形式で時刻を指定します。
image	イメージが再起動されるように設定します。
swap	アクティブなブート イメージを変更します。非アクティブなイメージを起動し、次の起動時にそこにデフォルト フラグを設定します。
no-swap	アクティブなイメージから起動します。
reset-aps	システムのリセット中にすべてのアクセス ポイントをリセットします。
save-config	（任意）システムのリセット前に設定を保存します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、2010-03-29 および 12:01:01 にシステムをリセットする例を示します。

```
(Cisco Controller) > reset system at 2010-03-29 12:01:01 image swap reset-aps save-config
```

reset system in

デバイスがリブートするまでの遅延時間を指定するには、**reset system in** コマンドを使用します。

reset system in HH : MM : SS image {**swap** | **no-swap**} **reset-aps save-config**

構文の説明

HH :MM :SS	遅延時間を指定します。
image	イメージが再起動されるように設定します。
swap	アクティブなブート イメージを変更します。非アクティブなイメージを起動し、次の起動時にそこにデフォルト フラグを設定します。
no-swap	アクティブなイメージから起動します。
reset-aps	システムのリセット中にすべてのアクセス ポイントをリセットします。
save-config	システムのリセット前に設定を保存します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、00:01:01 の遅延後、システムをリセットする例を示します。

```
(Cisco Controller) > reset system in 00:01:01 image swap reset-aps save-config
```

reset system cancel

スケジュールされたリセットを取り消すには、**reset system cancel** コマンドを使用します。

reset system cancel

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、スケジュールされたリセットを取り消す例を示します。

```
(Cisco Controller) > reset system cancel
```

reset system notify-time

スケジュールされたリセット前にトラップ生成を設定するには、**reset system notify-time** コマンドを使用します。

reset system notify-time *minutes*

構文の説明

minutes	スケジュールされた各リセットの何分前に、トラップを生成するか。

コマンド デフォルト

デフォルトでは、スケジュールされたリセットの 10 分前にトラップを生成するように設定されています。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、スケジュールされたリセットの 10 分前にトラップ生成を設定する例を示します。

```
(Cisco Controller) > reset system notify-time 55
```

reset peer-system

ピア コントローラをリセットするには、**reset peer-system** コマンドを使用します。

reset peer-system

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ピア コントローラをリセットする例を示します。

```
> reset peer-system
```

save config

コントローラの設定を保存するには、**save config** コマンドを使用します。

save config

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、コントローラの設定を保存する例を示します。

```
(Cisco Controller) > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
```

transfer download certpasswor

オペレーティング システムが Web アドミニストレーション SSL キーおよび証明書の暗号化を解除できるように、.PEM ファイルのパスワードを設定するには、**transfer download certpassword** コマンドを使用します。

transfer download certpassword *private_key_password*

構文の説明

private_key_password	証明書の秘密キーのパスワード。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、証明書の秘密キー パスワード certpassword を使用してファイルをスイッチに転送する例を示します。

```
(Cisco Controller) > transfer download certpassword
Clearing password
```

transfer download datatype

ダウンロードするファイル タイプを設定するには、**transfer download datatype** コマンドを使用します。

transfer download datatype {**avc-protocol-pack** | **code** | **config** | **eapdevcert** | **eapcacert** | **icon** | **image** | **ipseccacert** | **ipsecdevcert**| **login-banner** | **radius-avplist** |**signature** | **webadmincert** | **webauthbundle** | **webauthcert**}

構文の説明

avc-protocol-pack	システムに AVC プロトコル パックをダウンロードします。
code	システムに実行可能イメージをダウンロードします。
config	コンフィギュレーションファイルをダウンロードします。
eapcacert	システムに EAP ca 証明書をダウンロードします。
eapdevcert	システムに EAP dev 証明書をダウンロードします。
icon	システムに実行可能イメージをダウンロードします。
image	システムに Web ログイン ページをダウンロードします。
ipseccacert	システムに IPSec 認証局（CA） 証明書をダウンロードします。
ipsecdevcert	システムに IPSec dev 証明書をダウンロードします。
login-banner	コントローラのログイン バナーをダウンロードします。最大 1500 バイトのテキスト ファイルのみがサポートされます。
radius-avplist	FTP サーバから XML ファイル形式で RADIUS AVP をダウンロードします。
signature	システムにシグニチャ ファイルをダウンロードします。
webadmincert	システムに Web 管理の証明書をダウンロードします。

webauthbundle	システムにカスタム Web 認証バンドルをダウンロードします。
webauthcert	システムに Web ポータルの Web 証明書をダウンロードします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	**ipseccacert**、**ipsecdevcert**、および **radius-avplist** オプションが導入されました。

次に、システムに実行可能イメージをダウンロードする例を示します。

```
(Cisco Controller) > transfer download datatype code
```

transfer download datatype icon

コントローラ上に TFTP または FTP サーバからアイコンをダウンロードするには、**transfer download datatype icon** コマンドを使用します。

transfer download datatype icon

構文の説明	なし
コマンド デフォルト	なし
コマンド モード	WLAN の設定

コマンド履歴

リリース	変更内容
リリース 8.2	このコマンドが導入されました。

使用上のガイドライン

例

次に、コントローラ上に TFTP または FTP サーバからアイコンをダウンロードする例を示します。

```
Cisco Controller > transfer download datatype icon
```

transfer download filename

特定のファイルをダウンロードするには、**transfer download filename** コマンドを使用します。

transfer download filename *filename*

構文の説明

filename	ファイル名には、512 文字までの英数字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

\ : * ? " < > | のような特殊文字はファイル パスに使用できません。

次に、build603 という名前のファイルを転送する例を示します。

```
(Cisco Controller) > transfer download filename build603
```

transfer download mode

転送モードを設定するには、**transfer download mode** コマンドを使用します。

transfer upload mode {**ftp** | **tftp** | **sftp**}

構文の説明

ftp	転送モードを FTP に設定します。
tftp	転送モードを TFTP に設定します。
sftp	転送モードを SFTP に設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、TFTP モードを使用してファイルを転送する例を示します。

```
(Cisco Controller) > transfer download mode tftp
```

transfer download password

FTP転送用のパスワードを設定するには、**transfer download password** コマンドを使用します。

transfer download password *password*

構文の説明		
	password	パスワード。

コマンド デフォルト なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FTP 転送用のパスワードを pass01 に設定する例を示します。

```
(Cisco Controller) > transfer download password pass01
```

transfer download path

特定の FTP または TFTP パスを設定するには、**transfer download path** コマンドを使用します。

transfer download path *path*

構文の説明

path	ディレクトリ パス。 （注） TFTP または FTP サーバのパス名は、サーバのデフォルトまたはルート ディレクトリからの相対パスです。たとえば、Solarwinds TFTP サーバの場合、パスは「/」になります。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

\ : * ? " < > | のような特殊文字はファイル パスに使用できません。

次に、ファイルをパス c:\install\version2 に転送する例を示します。

```
(Cisco Controller) > transfer download path c:\install\version2
```

transfer download port

FTP ポートを指定するには、**transfer download port** コマンドを使用します。

transfer download port *port*

構文の説明

port	FTP ポート。

コマンド デフォルト

デフォルトの FTP ポートは 21 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

ch

次に、FTP ポート番号 23 を指定する例を示します。

```
(Cisco Controller) > transfer download port 23
```

transfer download serverip

情報をダウンロードする TFTP サーバの IP アドレスを指定するには、**transfer download serverip** コマンドを使用します。

transfer download serverip *ip-addr*

構文の説明

ip-addr	TFTP サーバの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、TFTP サーバの IPv4 アドレスを設定する例を示します。

```
(Cisco Controller) > transfer download serverip 175.34.56.78
```

次に、TFTP サーバの IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > transfer download serverip 2001:10:1:1::1
```

transfer download start

ダウンロードを開始するには、**transfer download start** コマンドを使用します。

transfer download start

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ダウンロードを開始する例を示します。

```
(Cisco Controller) > transfer download start
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 172.16.16.78
TFTP Path................................ directory path
TFTP Filename............................ webadmincert_name
This may take some time.
Are you sure you want to start? (y/n) Y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

transfer download tftpPktTimeout

TFTP パケットのタイムアウトを指定するには、**transfer download tftpPktTimeout** コマンドを使用します。

transfer download tftpPktTimeout *timeout*

構文の説明

timeout	秒単位でのタイムアウト（1 ～ 254）。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、55 秒の TFTP パケットのタイムアウトを設定してファイルを転送する例を示します。

```
(Cisco Controller) > transfer download tftpPktTimeout 55
```

transfer download tftpMaxRetries

許可する TFTP パケット再試行数を指定するには、**transfer download tftpMaxRetries** コマンドを使用します。

transfer download tftpMaxRetries *retries*

構文の説明

retries	1 ～ 254 秒の間で許可する TFTP パケット再試行数。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、許可する TFTP パケット再試行数を 55 に指定する例を示します。

```
(Cisco Controller) > transfer download tftpMaxRetries 55
```

transfer download username

FTP ユーザ名を指定するには、**transfer download username** コマンドを使用します。

transfer download username *username*

構文の説明

username	ユーザ名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に FTP ユーザ名を ftp_username に設定する例を示します。

```
(Cisco Controller) > transfer download username ftp_username
```

transfer encrypt

コンフィギュレーション ファイル転送の暗号化を設定するには、**transfer encrypt** コマンドを使用します。

transfer encrypt {**enable** | **disable** | **set-key** *key*}

構文の説明

enable	暗号化設定をイネーブルにします。
disable	暗号化設定をディセーブルにします。
set-key	コンフィギュレーション ファイル転送の暗号キーを設定します。
key	config ファイル転送の暗号キー。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、暗号化設定をイネーブルにする例を示します。

```
(Cisco Controller) > transfer encrypt enable
```

transfer upload datatype

指定したログおよびクラッシュ ファイルをアップロードするようにコントローラを設定するには、**transfer upload datatype** コマンドを使用します。

transfer upload datatype {**ap-crash-data** | **config** | **coredump** | **crashfile** | **debug-file** | **eapcacert** | **eapdevcert** | **errorlog** | **invalid-config** | **ipseccacert** | **ipsecdevcert** | **pac** | **packet-capture** | **panic-crash-file** | **radio-core-dump** | **radius-avplist** | **rrm-log** | **run-config** | **signature** | **systemtrace** | **traplog** | **watchdog-crash-filewebadmincert** | **webauthbundle** | **webauthcert**}

構文の説明

ap-crash-data	AP クラッシュ ファイルをアップロードします。
config	システム コンフィギュレーション ファイルをアップロードします。
coredump	コア ダンプ ファイルをアップロードします。
crashfile	システム クラッシュ ファイルをアップロードします。
debug-file	システムのデバッグ ログ ファイルをアップロードします。
eapcacert	EAP CA 証明書をアップロードします。
eapdevcert	EAP Dev 証明書をアップロードします。
errorlog	システム エラー ログ ファイルをアップロードします。
invalid-config	システムの無効なコンフィギュレーションファイルをアップロードします。
ipseccacert	CA 証明書ファイルをアップロードします。
ipsecdevcert	デバイス証明書ファイルをアップロードします。
pac	Protected Access Credential（PAC）をアップロードします。
packet-capture	パケット キャプチャ ファイルをアップロードします。
panic-crash-file	カーネル パニック情報ファイルをアップロードします。

radio-core-dump	システムエラー ログをアップロードします。
radius-avplist	コントローラからRADIUSサーバへXMLファイルをアップロードします。
rrm-log	システムのトラップ ログをアップロードします。
run-config	WLCの実行コンフィギュレーションをアップロードします。
signature	システム シグニチャ ファイルをアップロードします。
systemtrace	システム トレース ファイルをアップロードします。
traplog	システム トラップ ログをアップロードします。
watchdog-crash-file	クラッシュの後、ソフトウェア ウォッチドッグによって開始されるコントローラのリブートから生じるコンソールのダンプ ファイルをアップロードします。
webadmincert	Web 管理証明書をアップロードします。
webauthbundle	Web 認証バンドルをアップロードします。
webauthcert	Web 証明書をアップロードします。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	**ipseccacert**、**ipsecdevcert**、および **radius-avplist** オプションが導入されました。

次に、システム エラー ログ ファイルをアップロードする例を示します。

```
(Cisco Controller) > transfer upload datatype errorlog
```

transfer upload filename

特定のファイルをアップロードするには、**transfer upload filename** コマンドを使用します。

transfer upload filename *filename*

構文の説明

filename	最大 16 文字の英数字を含むファイル名。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

\ : * ? " < > | のような特殊文字はファイル パスに使用できません。

次に、ファイル build603 をアップロードする例を示します。

```
(Cisco Controller) > transfer upload filename build603
```

transfer upload mode

転送モードを設定するには、**transfer upload mode** コマンドを使用します。

transfer upload mode {**ftp** | **tftp** | **sftp**}

構文の説明

ftp	転送モードを FTP に設定します。
tftp	転送モードを TFTP に設定します。
sftp	転送モードを SFTP に設定します。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、転送モードを TFTP に設定する例を示します。

```
(Cisco Controller) > transfer upload mode tftp
```

transfer upload pac

ローカル認証機能をサポートする Protected Access Credential（PAC）をロードしてクライアントが PAC をインポートできるようにするには、**transfer upload pac** コマンドを使用します。

transfer upload pac *username validity password*

構文の説明

username	PAC のユーザ ID。
validity	PAC の有効期間（日数）。
password	PAC を保護するパスワード。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

クライアント アップロード プロセスでは TFTP または FTP サーバが使用されます。

次に、ユーザ名 user1、有効期限 53、およびパスワード pass01 である PAC をアップロードする例を示します。

```
(Cisco Controller) > transfer upload pac user1 53 pass01
```

transfer upload password

FTP 転送用のパスワードを設定するには、**transfer upload password** コマンドを使用します。

構文の説明

password	FTP サーバへのアクセスに必要なパスワード。

transfer upload password *password*

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FTP 転送用のパスワードを pass01 に設定する例を示します。

```
(Cisco Controller) > transfer upload password pass01
```

transfer upload path

特定のアップロード パスを設定するには、**transfer upload path** コマンドを使用します。

transfer upload path *path*

構文の説明

path	ファイルへのサーバ パス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

\ : * ? " < > | のような特殊文字はファイル パスに使用できません。

次に、アップロード パスを c:\install\version2 に設定する例を示します。

```
(Cisco Controller) > transfer upload path c:\install\version2
```

transfer upload peer-start

ピア WLC にファイルをアップロードするには、**transfer upload peer-start** コマンドを使用します。

transfer upload peer-start

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ピアのコントローラへのファイル アップロードを開始する例を示します。

```
(Cisco Controller) >transfer upload peer-start
Mode..................................... FTP
FTP Server IP.................................. 209.165.201.1
FTP Server Port................................ 21
FTP Path....................................... /builds/nimm/
FTP Filename................................... AS_5500_7_4_1_20.aes
FTP Username................................... wnbu
FTP Password................................... *********
Data Type...................................... Error Log

Are you sure you want to start upload from standby? (y/N) n

Transfer Canceled
```

transfer upload port

FTP ポートを指定するには、**transfer upload port** コマンドを使用します。

transfer upload port *port*

構文の説明

port	ポート番号。

コマンド デフォルト

デフォルトの FTP ポートは 21 です。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、FTP ポート番号 23 を指定する例を示します。

```
(Cisco Controller) > transfer upload port 23
```

transfer upload serverip

ファイルをアップロードするTFTPサーバのIPv4またはIPv6アドレスを設定するには、**transfer upload serverip** コマンドを使用します。

transfer upload serverip *ip-addr*

構文の説明

ip-addr	TFTP サーバの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。
8.0	このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

次に、TFTP サーバの IPv4 アドレスを 175.31.56.78 に設定する例を示します。

```
(Cisco Controller) > transfer upload serverip 175.31.56.78
```

次に、TFTP サーバの IPv6 アドレスを 175.31.56.78 に設定する例を示します。

```
(Cisco Controller) > transfer upload serverip 2001:10:1:1::1
```

transfer upload start

アップロードを開始するには、**transfer upload start** コマンドを使用します。

transfer upload start

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、ファイルのアップロードを行う例を示します。

```
(Cisco Controller) > transfer upload start
Mode..................................... TFTP
TFTP Server IP........................... 172.16.16.78
TFTP Path................................ c:\find\off/
TFTP Filename............................ wps_2_0_75_0.aes
Data Type................................ Code
Are you sure you want to start? (y/n) n
Transfer Cancelled
```

transfer upload username

FTP ユーザ名を指定するには、**transfer upload username** コマンドを使用します。

transfer upload username

構文の説明

username	FTP サーバへのアクセスに必要なユーザ名。ユーザ名には、最大31 文字を使用できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に FTP ユーザ名を ftp_username に設定する例を示します。

```
(Cisco Controller) > transfer upload username ftp_username
```

第 IX 部

Mobility Express コントローラ コマンド

• Mobility Express コントローラ コマンド （1907 ページ）

Mobility Express コントローラ コマンド

- アプリケーションの可視性コマンド （1908 ページ）
- ログ、コア、およびクラッシュ ファイルを収集するためのコマンド （1909 ページ）
- Cisco.com からソフトウェアをダウンロードするためのコマンド （1910 ページ）
- CleanAir コマンド （1911 ページ）
- CMX クラウド コマンド （1912 ページ）
- コントローラ イメージのアップグレード コマンド （1913 ページ）
- DNS コマンド （1914 ページ）
- 移行コマンド （1915 ページ）
- NTP コマンド （1916 ページ）
- 次の優先マスター AP と強制フェールオーバー （1917 ページ）
- UX 規制ドメイン コマンド （1918 ページ）
- VRRP コマンド （1919 ページ）
- WGB コマンド （1920 ページ）
- WLAN のセキュリティ コマンド （1921 ページ）

アプリケーションの可視性コマンド

次のコマンドは、Cisco Mobility Express コントローラのアプリケーションの可視性の設定に使用されます。

コマンド	説明	本リリースでの追加
config flexconnect group default-flexgroup avc 1 visibility { enable | disable }	WLAN のアプリケーションの可視性を有効化または無効化します	8.1.122.0
show flexconnect group detail default-flexgroup	各 WLAN のアプリケーションの可視性のステータスを表示します	8.1.122.0
show flexconnect avc statistics group default-flexgroup	FlexConnect グループに基づいたアプリケーション可視性の統計情報を表示します	8.1.122.0
how flexconnect avc statistics client *client_MAC*	各クライアントに基づいたアプリケーションの可視性の統計情報を表示します	8.1.122.0

ログ、コア、およびクラッシュファイルを収集するためのコマンド

コマンド	説明	本リリースでの追加
1. transfer upload datatype support-bundle **2.** transfer upload mode { tftp | ftp } **3.** transfer upload username *username* password *password* このコマンドは FTP 転送専用です。 **4.** transfer upload filename *filename* **5.** transfer upload path *file_path* **6.** transfer upload serverip *server_ip_address* **7.** transfer upload start	これらのコマンドを順番に使用して、ログ、コア、およびクラッシュファイルを収集します。 次のデータ タイプのファイルが収集され、.TAR ファイルにまとめられて、設定済みの TFTP または FTP サーバにアップロードされます。 • run-config • systemtrace • traplog • debug-file • crashfile • coredump • ap-crash-data	8.3.102.0
debug transfer all enable	コードフローをデバッグするには、**transfer upload start** コマンドの前にこのコマンドを使用します。	8.3.102.0
debug disable-all	コードフローのデバッグを無効にします。	8.3.102.0

Cisco.comからソフトウェアをダウンロードするためのコマンド

ステップ	コマンド	説明	本リリースでの追加
1	transfer download ap-images mode cco	Cisco.com からソフトウェアイメージのダウンロードするモードを設定します。	8.3.102.0
2	transfer download ap-images cco-username *username* cco-password *password*	Cisco.com の資格情報を使用するよう指定します。	8.3.102.0
3	transfer download ap-images version { suggested | latest }	推奨されるソフトウェアバージョンのイメージをダウンロードするか、最新のソフトウェアバージョンのイメージをダウンロードするかを指定します。	8.3.102.0
4	transfer download ap-images cco-auto-check { enable | disable }	Cisco.com からのソフトウェアイメージの更新を自動的にチェックするようコントローラを設定します。	8.3.102.0
5	transfer download start	ダウンロードを開始します。	8.3.102.0

CleanAir コマンド

コマンド	説明	本リリースでの追加
config 802.11b cleanair enable *ap_MAC*	関連する AP で CleanAir を有効化します。1850 および 1830 シリーズ AP には適用されません。	8.1.122.0
show 802.11b cleanair device ap *ap_MAC*	AP に接続しているすべての干渉デバイスを表示します。	8.1.122.0
show 802.11b cleanair device type jammer	特定の干渉デバイスを電波妨害します。	8.1.122.0

CMX クラウド コマンド

コマンド	説明	本リリースでの追加
config cloud-services server id-token *CMX_token*	有効なCMXサーバのトークンを指定します。	8.3.102.0
config cloud-services server url *url*	有効な CMX サーバの URL を指定します。	8.3.102.0
config cloud-services cmx enable	CMX 分析を有効にします。	8.3.102.0
show cloud-services cmx summary	設定されているCMXクラウド サービスの詳細を表示します。	8.3.102.0

コントローラ イメージのアップグレード コマンド

次のコマンドは、Mobility Express コントローラ ソフトウェア イメージのアップグレードを実行する場合に使用されます。

コマンド	説明	本リリースでの追加
transfer download ap-images imagePath *image_path*	TFTP サーバのソフトウェア イメージのパスを設定します	8.1.122.0
transfer download ap-images mode tftp	ファイル転送モードを TFTP に設定します	8.1.122.0
transfer download ap-images serverIp *ipv4_address*	TFTP サーバの IP アドレスを指定します	8.1.122.0
transfer download start	設定を保存し、イメージのダウンロードを開始します	8.1.122.0
transfer download stop	進行中のイメージのダウンロードを停止します	8.3.102.0
debug transfer all { enable | disable }	有効になっているすべてのサブ コマンドを使用して転送とダウンロードをデバッグします	8.1.122.0
debug transfer tftp { enable | disable }	TFTP の転送ダウンロードをデバッグします	8.1.122.0
debug transfer trace { enable | disable }	転送トレースをデバッグします	8.1.122.0

DNS コマンド

コマンド	説明	本リリースでの追加
config network dns default	デフォルト DNS サーバを設定します。	8.2.100.1
show network summary	デフォルト DNS サーバ（有効の場合）がリストされているネットワーク概要を表示します。	8.2.100.1

移行コマンド

次のコマンドは、Mobility Express ソフトウェア イメージから Lightweight CAPWAP AP ソフトウェア イメージに AP を変換する場合、およびその反対に変換する場合に使用されます。

コマンド	説明	本リリースでの追加
ap-type capwap	Mobility Express から CAPWAP に AP タイプを変換します	8.1.122.0
ap-type mobilityexpress tftp://*tftp_server*/*file_name*	Mobility Express ソフトウェア イメージの実行時に CAPWAP から Mobility Express に AP タイプを変換します	8.1.122.0
config ap unifiedmode *switch_name switch_IP_address*	すべてのAPをスイッチからCAPWAPにタイプを同時に変換します	8.1.122.0

NTP コマンド

コマンド	説明	本リリースでの追加
config time ntp server 1 *FQDN_of_server*	NTP サーバ（ここでは例として、NTP インデックス 1 を持つ）の完全修飾ドメイン名を設定します。	8.2.100.1
config time ntp server 2 *NTP_Server_IP_address*	NTP サーバ（ここでは例として、NTP インデックス 2 を持つ）の IP アドレスを設定します。	8.2.100.1

次の優先マスター AP と強制フェールオーバー

コマンド	説明	本リリースでの追加
config ap next-preferred-master *cisco_ap_name*	次の優先マスターAPを設定します。	8.3.102.0
config ap next-preferred-master *cisco_ap_name* forced-failover	次の優先マスターAPを設定し、そのAPへのフェールオーバーを手動でトリガーします。	8.3.102.0

UX 規制ドメイン コマンド

コマンド	説明	本リリースでの追加
config wlan disable 1	WLAN 1 を無効にします	8.1.122.0
config wlan universal-ap-admin enable 1	WLAN 1 のユニバーサル AP 管理者として有効化します	8.1.122.0
config wlan enable 1	WLAN 1 を有効にします	8.1.122.0
show ap summary	UX ではない場合、設定されている現在の国（US、IN など）を表示します	8.1.122.0

VRRP コマンド

次の Virtual Router Redundancy Protocol（VRRP）コマンドは、Mobility Express コントローラのフェールオーバー時にマスター AP のために使用されます。

コマンド	説明	本リリースでの追加
config ap next-preferred-master	新しいマスターAPとして引き継ぐために選択されたマスターAPを設定します	8.1.122.0
show ap next-preferred-master	マスターAPの状態を表示します	8.1.122.0
clear ap next-preferred-master	マスターAPの設定をクリアします	8.1.122.0
show mob-exp vrrp vrid	VRID を表示します。	8.8.100.0
show mob-exp vrrp vrid	VRRP MAC を表示します	8.8.100.0

WGB コマンド

次の show コマンドはワークグループ ブリッジ（WGB）の詳細を表示するために使用できます。

コマンド	説明	本リリースでの追加
show wgb summary	ワークグループ ブリッジの概要を表示します	8.1.122.0
show wgb detail *WGB_MAC*	特定のワークグループ ブリッジの詳細を表示します	8.1.122.0

WLAN のセキュリティ コマンド

コマンド	説明	本リリースでの追加
config wlan security wpa akm cckm {enable | disable} wlan_id	CCKM の有効化または無効化	8.2.100.1

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。